TEKNILLINEN KORKEAKOULU
Sähkötekniikan osasto

Juha Korhonen

# Laajojen Windows työasemaverkkojen tietoturvan ja konfiguraationhallinnan toteuttaminen

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 06.12.1995

Työn valvoja — Professori Heikki Saikkonen

Työn ohjaaja — DI Pauli Hovinen

# Tiivistelmä

Tekijä: Juha Korhonen

Työn nimi: Laajojen Windows työasemaverkkojen tietoturvan ja konfiguraationhallinnan toteuttaminen

Päivämäärä: 06.12.95 Sivumäärä: 91

Osasto: Sähkötekniikan osasto

Professuuri: Tietojenkäsittelyoppi

Työn valvoja: Professori Heikki Saikkonen

Työn ohjaaja: DI Pauli Hovinen

Erilaiset tietojärjestelmät ja tietokonelaitteistot ovat saavuttaneet tärkeän osan yhteiskunnassamme. Tietokoneita käytetään työskentelyssä miltei kaikilla elämän aloilla. Tietokoneiden käytön lisäytyessä myös tietoturvan merkitys korostuu. Tietoturvan lisäksi työasemien konfiguraationhallinta on muodostunut tärkeäksi. Tehokkaalla konfiguraationhallinnalla saavutetaan suurempi käyttöaste ja helpotetaan käyttäjien työtä. Tällä on mahdollista saavuttaa huomattavia kustannussäästöjä.

Tietokoneissa on siirrytty isoista suurkoneista pienempiin mikrotietokoneisiin. Ylläpitäjien työmäärä on samalla moninkertaistunut, koska keskitettyä ylläpitoa on ollut vaikea tehdä. Mikrotietokoneiden yleisin käyttöjärjestelmä on Microsoft Windows. Windowsin suunnittelussa tietoturva ei ole ollut päällimmäisenä ja siinä on suuria puutteita.

Tämän työn tarkoituksena oli kartoittaan Windowsin turvallisuuden ja konfiguraationhallinnan puutteita, etsiä ja toteuttaa ratkaisu, jolla Windows-työasemia pystytään käyttämään turvallisesti. Työaseman turvallisuustavoitteeksi asetettiin ITSEC:in C2 turvallisuustaso. Ylläpitäjien ja käyttäjien työmäärää helpottamaan toteutetaan konfiguraationhallinta, joka mahdollistaa saman työaseman tehokkaan jakamisen eri käyttäjien välillä, käyttäjien henkilökohtaisen konfiguraation seuraamisen työasemasta toiseen ja ohjelmien automaattisen asentamisen.

Avainsanat: Windows, C2, tietoturva, konfiguraationhallinta

# Abstract

Author: Juha Korhonen

Name of the thesis: Computer security and configuration management for Windows based computer networks

Date: 06.12.95 Number of pages: 91

Faculty: Faculty of Electrical Engineering

Professorship: Computer science

Supervisor: Professor Heikki Saikkonen

Instructor: M.Sc. Pauli Hovinen

Different kind of information and computer systems have gained an important role in our society. Nowadays computers are used pretty much in every field of life. As the computer systems have gained more important role, also the computer security has became more important. Another topic that has became more important lately is configuration management. Efficient configuration management keeps computer systems available and that way makes users job more easier. It's also makes possible to gain big savings

Computer system have changed from big mainframes to small personal computer systems. That has caused more work to administrators, because it's very difficult to have centralised management. Microsoft Windows is the most common operating system in PC-computers. Computer security was not any of the main focuses while Windows was made, and there are big problems with it.

Purpose of this work was to map security and configuration management problems in Windows, seek and implement solution, that makes Windows workstations safe. Security goal was chosen to be ITSEC C2-security criteria. Workstation will be made easier to use both to administrators and users by implementing a configuration management. It will be possible to configure workstations from one place, users may share same workstation efficiently, users configurations will follow them from workstation to another and administrators can automatically install new software.

Keywords: Windows, C2, computer security, configuration management

# Alkulause

Tämä diplomityö on tehty ICL Personal Systems Oy:ssä Desktop Products-ryhmässä, Helsingissä.

Työn valvojana toimi professori Heikki Saikkonen ja työtäni ohjasi DI Pauli Hovinen, joille molemmille esitän kiitokseni.

Erityisesti haluan kiittää työtoveriani Antti Saarenheimoa, joka jaksoi omien kiireidensä ohella syventyä myös keskustelemaan DeskTop:sta

Juha Korhonen

Espoossa 06.12.95

# Sisällysluettelo

# Lyhenteitä ja käsitteitä

| | |
|---|---|
| API | Application programming interface |
| BIOS | Basic Input Output System |
| DDE | Dynamic Data Exchange |
| DLL | Dynamically Linked Library, ajonaikainen kirjasto. Kirjastoa ei ole kiinteästi sidottu ohjelmaan, vaan se ladataan ajonaikana muistiin. Jos useat ohjelmat haluavat käyttää samaa DLL:ää, ne kaikki käyttävät samaa kopiota muistissa, eikä niitä tarvitse ladata useita muistiin. |
| FAT | File allocation table, Dos:in käyttämä tiedostojärjestelmä |
| HLL | High Level Language |
| HPFS | High performance filesystem, OS/2 käyttämä tiedostojärjestelmä |
| INI-tiedostot | Konfiguraatiotietoa sisältävät tiedostot, joiden loppupääteenä on .ini. |
| ITSEC | Information Techonology Security Evaluation Criteria |
| ROM | Read Only Memory. Muisti jonne tallennetua tietoa voidaan vain lukea. |
| NTFS | NT-file system, Windows NT:n käyttämä tiedostojärjestelmä |
| NDS | NetWare Directory Services, Netwaren käyttämä puumainen rakenne verkkoresursseille |
| TCSEC | Trusted Computer System Evaluation Criteria |
| Villikortit | Jokerimerkit, korvausmerkit (wild cards). Erikoismerkkejä, joita käytetään korvaamaan merkkejä ja merkkijonoja. Villikortteja on ? ja *. ?-merkki korvaa yhden merkin, *-merkki korvaa ueita merkkejä. |
| ZSIC | Saksan kansallinen turvallisuuskriteeri |

# 1. Johdanto

Tietoturvan merkitys on viime vuosina korostunut ja samalla siihen on alettu kiinnittää yhä enemmän huomiota. Yritykset ja yhteisöt ovat pitkälle riippuvaisia tietojärjestelmistään eikä ole yhdentekevää, miten luotettavasti järjestelmät toimivat tai kuka niihin pääsee käsiksi. Työt joita ennen tehtiin käsin kynällä ja paperilla, tehdään nyt tietokoneen avustuksella. Jos tietokoneet eivät jostain syystä ole käytettävissä, ei myöskään pystytä tekemään töitä. Lisäksi tietokoneissa pidetään paljon luottamuksellista materiaalia - tietoa, jonka joutuminen esimerkiksi kilpailijan käsiin on hyvin vahingollista. Myös omat työntekijät voivat tahtomattaan tai tahallaan aiheuttaa vahinkoa yrityksen tietojärjestelmälle. Näitä uhkia on pystyttävä hallitsemaan ja ehkäisemään.

Tietokoneiden kehitys on kulkenut poispäin suur- ja minikonejärjestelmistä. Niiden tilalle ovat tulleet henkilökohtaiset mikrotietokoneet ja asiakas-palvelin-ratkaisut. Laskentatehon ja hinnan suhde kasvaa nopeimmin juuri mikrotietokoneissa, ja samalla suurin osa uusista sovelluksista tehdään niille.

Suurkone-järjestelmissä oli käytössä vain yksi tai muutamia tietokoneita, joita käytettiin päätteiden kautta. Tietokoneella oli palkattuna ylläpitäjä, jonka tehtävänä oli tietokoneen käyttökunnossa pitäminen. Ylläpitäjä huolehti myös uusien ohjelmien asentamisesta ja piti huolta siitä, että tietokoneen konfiguraatio oli kunnossa. Tilanne kuitenkin muuttuu oleellisesti, kun ei olekaan enää vain muutama tietokone, vaan koneita on kymmeniä tai satoja. Edelleen on olemassa ylläpitäjä, mutta hän ei pysty enää huolehtimaan kaikista koneista yhtä hyvin. Jos tapahtuu jotain mikä sotkee useita koneita samanaikaisesti, joku joutuu pakostakin odottelemaan, että ylläpitäjä ehtii korjaamaan ongelman.

Microsoft Windows on tällä hetkellä mikrotietokoneiden käyttöjärjestelmien markkinajohtaja. Siitä on tullut standardikäyttöjärjestelmä toimistokäyttöön tarkoitetuissa mikrotietokoneissa. Windowsia suunniteltaessa turvallisuus- ja hallittavuusnäkökohdat eivät kuitenkaan olleet päällimmäisinä, ja siksi Windowsissa on varsin pahoja puutteita. Paketista otettu Windows ei tarjoa turvallisuuden kannalta oikeastaan mitään. Käyttäjät voivat tehdä melkein mitä tahansa jättämättä minkäänlaisia jälkiä.

Tämän työn tarkoituksena oli löytää ratkaisu Windowsin turvallisuus- ja hallinta ongelmiin, mahdollistaa ylläpitäjille työasemaverkkojen keskitetty hallinta ja helpottaa ohjelmistojen asentamista.

# 2. Tietoturva

Samalla kun erilaiset tietojärjestelmät ovat saavuttaneet tärkeän, usein jopa elintärkeän roolin yhteiskunnan eri alueilla, on myös tietoturvasta tullut olennainen osa tietojärjestelmää. Tietoturvan merkitys myönnetään, mutta siihen ei välttämättä olla halukkaita investoimaan.

## *Uhkatyypit*

Tietojärjestelmiin kohdistuvat uhat voidaan jakaa kolmeen pääryhmään: luonnolliset, tahattomat ja tahalliset /1/.

Luonnollisia uhkia ovat luonnosta ja ympäristöstä johtuvat asiat. Tulipalot, tulvat, sähkökatkokset ja muut katastrofit voivat helposti hajottaa tietokoneet. Vaikka näitä uhkia on varsin vaikea estää kokonaan, voidaan kuitenkin huolehtia siitä, että ne havaitaan nopeasti ja niiden aiheuttamat vahingot minimoidaan. (Palohälyttimet, varavoimalähteet jne.) Varmuuskopiot säilytetään paloturvallisissa kaapeissa ja tarvittaessa kopioidaan säilytettäväksi toiseen paikkaan..

Tahattomia uhkia tietojärjestelmille ovat usein niiden tavalliset käyttäjät. Esimerkiksi ylläpitäjä, joka ei ymmärrä tietoturvan merkitystä, koska häntä ei ole koulutettu kunnolla tai joka ei ole lukenut ohjeita voi vahingossa aiheuttaa aukkoja järjestelmään. Käyttäjä voi yrittää asentaa uutta ohjelmaa ja erehdyksessä tuhota tärkeitä tiedostoja. Useat ohjelmat mahdollistavat tiedon tuhoamisen tai hävittämisen ihan tavallisessa käyttötilanteessa, jos käyttäjä ei tiedä mitä tekee.

Tahalliset uhat ovat niitä, jotka yleensä ylittävät uutiskynnyksen. Turvallisuustuotteet ovatkin yleensä suunnattu juuri tahallisia uhkia vastaan. Tahallisella uhalla tarkoitetaan, että joku yrittää tarkoituksella päästä käsiksi tietoon, johon hänellä ei ole oikeutta tai yrittää käyttää resurssia, joka ei ole hänelle sallittua. Tahalliset uhat voidaan jakaa vielä kahteen ryhmään: sisäisiin ja ulkoisiin. Ulkoiset uhat ovat yrityksen ulkopuolella olevia tahoja, jotka jostain syystä yrittävät päästä käsiksi yrityksen tietojärjestelmiin. Näitä tahoja ovat esimerkiksi:

- Ulkomaalaiset tiedustelupalvelut. Tiedustelupalvelut ovat harvoin kiinnostuneita tavallisista yrityksistä, mutta esimerkiksi eri valtioiden puolustusvoimille ne ovat olemassa oleva ja vakavasti otettava uhka.

- Terroristit. Onneksi tietokoneterrorismia ei ole vielä juurikaan esiintynyt. On ollut muutamia harmittomia tapauksia, joissa on hyökätty yliopiston tietokonekeskuksiin, armeijan värväystoimistoihin tai oikeussaleihin. USA:n valtio on huolissaan /1 s14-17/ mahdollisesta tietokoneterrorismistä, samoin kuin lentoyhtiöt, öljy-yhtiöt ja muut yritykset, jotka voivat joutua terrorismin kohteeksi.

- Rikolliset. Tietojärjestelmät ovat otollisia kohteita rikollisille. Toisin kuin rikokset yleensä, näitä rikoksia on mahdollista tehdä kaukaa. Tavoitteena voi olla varkaus tai vaikkapa taloudellisen vahingon tuottaminen.

- Teollisuusvakoilijat. Tietojärjestelmä on hyvä kohde teollisuusvakoilulle. Tietojärjestelmässä säilytetään yrityksen suunnitelmia ja muita tärkeitä papereita. Yritysjohdon sähköpostiviestit ja muistiot ovat rahanarvoista tavaraa kilpailijalle.

Sisäiset uhat ovat puolestaan yrityksen oman henkilökunnan aiheuttamia. Heillä ei ole ongelma päästä käsiksi laiteisiin tai päästä sisälle rakennuksiin. On arvioitu, että jopa 80% järjestelmien väärinkäytöksistä tapahtuu oman henkilökunnan toimesta. Myös sisäiset uhat voidaan jakaa erilaisiin ryhmiin. Erotettu työntekijä voi yrittää varastaa yrityksen tietoja tai pahimmassa tapauksessa aiheuttaa tuhoa. Työntekijää voidaan myös kiristää ja pakottaa tekemään jotain mitä hän ei halua. Ahne työntekijä voi yrittää käyttää yrityksen tietoja omaksi edukseen. Usein vakavin sisäinen uhka on tietämätön työntekijä, joka ei vaivaudu vaihtamaan salasanaansa riittävän usein tai ei opettele käyttämään tiedostojen salausta. Näistä aukoista epärehellinen taho pääsee helpommin käsiksi tietojärjestelmään.

Merkittävä osa tietoturvasta voidaan toteuttaa ilman mitään uusia laitteita tai koneita. Tietoturvaa voidaan parhaiten kehittää kouluttamalla henkilökuntaa ja saamalla heidät huomaamaan tietoturvan merkitys. Hyvin usein ihmiset ajattelevat, että puheet tietoturvasta ovat liioittelua tai ettei asia heitä kosketa.

Käyttäjien tekemät virheet, tietämättömyys turvallisuusriskeistä ja järjestelmävirheet muodostavat suurimman osan turvallisuusriskeistä. Seuraavana tulevat tarkoitukselliset väärinkäytöt ja hyvin pienenä joukkona ovat alan ammattilaisten tekemät "murrot", joissa käytetään erityisiä laitteita ja ohjelmistoja.

### *Suojautuminen*

Erilaiset uhat vaativat erilaisia suojatoimia. Luonnon uhkia vastaan voi suojautua erilaisissa varoituslaitteilla. Tulvia ja myrskyjä ei voi estää, mutta niiden aiheuttamia

vahinkoja voi yrittää minimoida. Ulkoisia uhkia vastaan voi suojautua fyysisillä suojatoimilla. Tilat voi rakentaa niin, että ulkopuoliset eivät niihin pääse. Lukot, kulkukortit ja jopa erilaiset fyysiset tunnistuslaitteet (sormenjäljet, ääni, käsiala ja silmän verkkokalvo) estävät asiattomia pääsemästä tiloihin ja mahdollistavat myös sen, että voidaan pitää silmällä ketkä omasta henkilökunnasta käyvät tiloissa.

Tietoliikenne pitää myös suojata. Tarvitaan erilaisia "palomuureja" (firewall) suojaamaan yrityksen tietoverkkoa ulkopuolisilta tunkeutujilta. Palomuurilla tarkoitetaan, että sisäinen verkko erotetaan ulkopuolisesta verkosta erillisellä hyvin suojatulla tietokoneella, ja kaikki yhteydet ulkopuolella ohjataan tämän palomuurikoneen kautta. Suorat yhteydet estetään. Luottamukselliset viestit pitää kuljettaa salattuna, ja ulkopuolelta tulevia yhteyksiä pitää pystyä valvomaan ja kontrolloimaan.

Perinteisesti tietokoneen tietoturvalla on käsitetty tietokoneessa ajettavien käyttöjärjestelmien ja sovellusohjelmien turvallisuusominaisuuksia: käyttäjien pääsyä tietojärjestelmään valvotaan ja kontrolloidaan, sekä pidetään kirjaa tapahtumista. Myös ohjelmien suorittaminen voi vaatia erilaisia oikeuksia, ja tiedostoilla on oikeudet mikä määrittää kuka saa lukea/muuttaa tiedostoa.

## 2.1. Tietoturvan osa-alueet

Information Technology Security Evaluation Criteria (ITSEC) määrittelee tietoturvan seuraaviin alueisiin /2 s.1-2/:

- Luottamuksellisuus, pidetään huolta siitä, että tietoon ei pääse luvattomasti käsiksi.
- Eheys, huolehditaan siitä, että tietoa ei voida luvattomasti muuttaa.
- Saavutettavuus, pidetään huolta siitä, että tieto tai palvelu on tarvittaessa käytettävissä.

Luottamuksellisuus tarkoittaa että järjestelmä pitää huolta etteivät luvattomat tahot pääse käsiksi tietoon, johon niillä ei ole oikeutta. Sen ominaisuuksiin kuuluvat mm. autentikointi - kaikki järjestelmän käyttäjät ovat tunnettuja. Lisäksi eri käyttäjillä ja tiedoilla pitää olla määritellyt oikeudet.

Eheys tarkoittaa, että käyttäjän on pystyttävä luottamaan tiedon aitouteen, siihen ettei tietoa ole kukaan voinut muuttaa.

Turvallisen tietokonejärjestelmän täytyy pystyä pitämään tieto käyttäjien saatavilla. Saavutettavuudella tarkoitetaan että tietokonejärjestelmän laitteisto ja ohjelmisto toimii tehokkaasti ja pystyy toipumaan nopeasti ja täydellisesti jos virheitä tapahtuu.

Saavutettavuuden vastakohta on palvelun estäminen. Se tarkoittaa, että järjestelmän käyttäjät eivät pysty käyttämään tarvitsemiaan resursseja. Tietokone on saattanut kaatua, käytettävissä ei ole tarpeeksi muistia tai tarvittavat levyt tai kirjoittimet eivät ole toiminnassa. Palvelun kieltäminen voi olla ihan yhtä paha uhka kuin tietovarkauskin. Esimerkiksi vuonna 1988 internetissä riehunut tietokonemato (Worm) ei itse asiassa hävittänyt tai tuhonnut tietoa, vaan se tukki tietokoneet luomalla uusia prosesseja ja leviämällä tietoverkkoja pitkin niin, että tietokoneilla ei voinut tehdä mitään hyödyllistä.

Eräällä tavoin saavutettavuus on perusturvallisuutta, jota kaikki tarvitsevat. Usein ei vain tulla ajatelleeksi, että tietokoneiden pitäminen toimintakunnossa on myös erääntyyppistä tietoturvaa.

Tietoturvan ongelmana on, että se tekee helposti järjestelmän käyttämisen monimutkaiseksi. Hyvän ja turvallisen järjestelmän tulee olla myös helppokäyttöinen. Turvallisuuden ei pitäisi aiheuttaa käyttäjille kohtuutonta haittaa.

## 2.2. Tietoturvastandardit

Tietojärjestelmien ostajat ja käyttäjät tarvitsevat tietoa siitä, miten hyvä heidän tietoturvansa on. Puolueettoman tiedon saaminen on kuitenkin ongelmallista. Tuotteiden valmistajat eivät halua kertoa tuotetta myydessään sen huonoista puolista, ja toisaalta isojen järjestelmien evaluointi itse on vaikeaa ja kallista. Myös erilaisten järjestelmien vertaaminen toisiinsa on hankalaa. Eri tuotteet eroavat usein varsin vähän tai sama asia on totetutettu toiminnallisesti aivan eri tavalla. Samantyylisten ratkaisujen vertailu on vaikeaa. Vertailu helpottuu, jos vertailtavat järjestelmät noudattavat yhteisiä standardeja tai ne on evaluoitu samojen kriteerien mukaan. Käyttäjän tai ostajan on myös helpompaa luottaa valmistajan ilmoituksiin, jos järjestelmän on testannut jokin kolmas osapuoli.

Evaluointi ja testaaminen vaatii hyvin määritellyt ohjeet ja standardit siitä, mitä turvallisuus kyseisessä tapauksessa tarkoittaa ja sisältää. Samalla tulee määritellyksi, mikä on kyseisen järjestelmän turvallisuustavoite ja mitä tuote itseasiassa tekee ja miltä se suojaa. Jotta eri tuotteiden vertaaminen olisi mielekästä ja mahdollista, pitää myös määritellä, mitä ja miten niitä testataan. Saatavien tulosten tulee olla mahdollisimman yksiselitteisiä ja helposti verrattavissa.

Tietojärjestelmien turvallisuuden evaluointimenetelmiä ja ohjeita on kehitetty jo kauan aikaa. Vaikkakin vaatimukset vaihtelevat jonkin verran riippuen siitä, mikä on kohdealue tai mitä asioita eri maat tai osapuolet ovat halunneet painottaa, on näissä myös paljon yhteisiä tekiöitä. Epäilemättä tärkein näistä ja yksi ensimmäisistä ohjeista on "Trusted Computer System Evaluation Criteria" [TCSEC], joka on yleisesti tunnettu joko TCSEC:inä tai ns. Orange Book:ina. Tämän ohjeen on julkistanut USA:n puolustusministeriö (Department of Defence). Monet muut maat, varsinkin eräät Euroopan maat ovat myös kunnostautuneet turvallisuusohjeiden tekemisessä. Englannissa on kehitetty valtion käyttöön CESG Memorandum Number 3, ja tehty kauppa- ja teollisuusministeriön suositus kaupallisten turvallisuustuotteiden evaluointiin ns. "Green Book". Saksa on julkistanut oman ohjeensa 1989 ja samaan aikaan myös Ranskassa kehiteltiin vastaavaa ohjetta. ("Blue-White-Red Book"). /2 s2-3/

Euroopassa huomattiin, että hyvin samankaltaista kehitystä oli tapahtumassa useissa maissa samanaikaisesti, ja tiedettiin myös tehtävää olevan vielä paljon. Ranska, Saksa, Hollanti ja Englanti päättivät tehdä yhteisen tietoturvallisuusohjeen. Ajatuksena oli yhdistää alan kokemusta eri maista. Lisäksi teollisuuden kannalta on hyvin huono asia, jos eri maissa on omat erilaiset turvallisuusstandardit. Perusajatukset kaikissa standardissa olivat samat. Menetelmien yhtenäisyys olisi etu kaikille (mm. erilaisille

teollisuuden, valtion ja puolustusvoimien sovelluksille). Turvallisuusstandardin nimeksi tuli ITSEC ( Information Technology Security Evaluation Criteria ).

Uutta turvallisuuskriteeriä suunniteltaessa haluttiin ylläpitää yhteensopivuutta jo olemassa olevien kriteerien kanssa, joista tärkein oli USA:n TCSEC. Vaikka alunperin tarkoituksena olikin lähinnä yhtenäistää jo käytössä olevia kriteerejä, huomattiin, että joissain asioissa kriteerejä oli tarvetta laajentaa.

## 2.2.1. ITSEC-kriteeri

Tärkein syy yhtenäisen standardin tekemiselle oli halu tehdä vertailukelpoinen pohja, jota voitaisiin käyttää mallina kansallisten turvallisuusohjeiden tekemiselle, ja joka mahdollistaisi eri maissa tehtyjen tuotteiden vertailun.

*ITSEC-kriteeri määrittelee, mikä on testattava kohde, mikä on sen toiminnallisuus, ja miten sen oikeellisuus varmennetaan, sekä määrittelee erilaisia turvallisuustasoja.* /2/

Kohde voi olla joko järjestelmä tai tuote. Erona on se, mitä voidaan sanoa varmasti niiden tulevasta käyttöympäristöstä. Järjestelmä on suunniteltu täyttämään tietyn loppukäyttäjäryhmän vaatimukset. Sillä on olemassa tunnettu ympäristö, joka voidaan määritellä yksityiskohtaisesti; erityisesti loppukäyttäjät ja heidän vaatimuksensa ovat tunnettuja, ja turvallisuusuhat voidaan määrittää. Tuote puolestaa toimii erilaisissa järjestelmissä. Tuotteen suunnittelija voi tehdä vain osittaisia arvioita lopullisesta käyttöympäristöstä. Tuotteen ostaja rakentaa lopullisen järjestelmän ja varmistaa, että tuotteen suunnitelussa tehdyt oletukset ovat riittäviä myös lopulliselle ympäristölle.

Sekä järjestelmiin että tuotteisiin käytetään samoja kriteerejä. Se on tärkeää siksi, että on helpompaa ja halvempaa evaluoida systeemejä, joiden käyttämät tuotteet on evaluoitu samojen kriteerien mukaan.

Evaluoinnin teettää evaluoinnin sponsori ja sen tekee ulkopuolinen evaluointitaho. Se testaa evaluoinnin kohteen, ja antaa tuloksena raportin evaluoinnista.

## 2.2.2. Turvallisuusvaatimukset ja evaluointitasot

Evaluoinnin kohteella on oltava tunnetut turvallisuusvaatimukset. Näitä vaatimuksia ovat esimerkiksi pääsyn valvonta, auditointi ja toipuminen virheistä. Nämä funktiot on määriteltävä yksiselitteisesti niin, että sekä evaluoinnin tekijä että sen sponsori ovat samaa mieltä siitä, mitä mikin turvallisuusvaatimus tarkoittaa. ITSEC:in kriteerissä esitetään kymmenen erilaista toiminnallista esimerkkiluokkaa. Nämä esimerkkiluokat

perustuvat Saksan kansallisesta kriteeristä (ZSIC) ja USA:n TCSEC:istä valittuun viiteen toiminnallisten vaatimusten esimerkkiin.

Evaluointitasot määrittelevät sen, miten evaluointi suoritetaan, ja mitä dokumentteja tuotteesta on oltava. ITSEC määrittelee seitsemän eri evaluointitasoa. Evaluointitason tehtävänä on kertoa, miten hyvin on varmistettu se, että tuote täyttää sille asetetut toiminnalliset vaatimukset. Eri tasot on nimetty E0:sta E6:seen. Mitä suurempi luokka, sitä enemmän voidaan luottaa siihen, että toiminnallisuus myös toimii niin kuin pitää. Tämä oikeellisuus kattaa koko evaluoinnin kohteen valmistamisen kehitysprosessista ja -ympäristöstä aina kohteen toimintaan. Korkeimmilla evaluointitasoilla ohjelmien oikeellisuus pitää todistaa formaalisti tai semi-formaalisti, kun taas matalammilla tasoilla tuotetta testataan.

Oikeellisuuden lisäksi tutkitaan ominaisuuden tehokkuus; kuinka hyvin ominaisuus suojaa määriteltyä uhkaa vastaan - ja miten hyvin se kestää sitä vastaan suunnattuja suoria hyökkäyksiä.

### 2.2.3. Evaluointiprosessi

*Evaluointiprosessin tarkoituksena on tuottaa raportti, jossa kerrotaan täyttääkö kohde sille määritellyt turvallisuusvaatimukset sillä oikeellisuuden tasolla, mikä on määritelty valitulla evaluointitasolla.*

ITSEC määrittelee tarkasti, mitä dokumentteja sponsorin on toimitettava ja miten evaluointi suoritetaan. Yleensä järjestelmien evaluoinin sponsorina toimii järjestelmän ostaja tai heidän tekninen edustajansa kun taas tuotteiden sponsorina toimii tuotteen valmistaja. Kaikki, jotka pystyvät toimittamaan tarvittavan teknisen informaation, voivat toimia sponsorina.

Mitä korkeampi valittu evaluointitaso on, sitä enemmän sponsorin ja evaluoijan on toimittava yhdessä. Aluksi sponsori määrittää toiminnallisen ympäristön ja ne uhat, jotka kohdistuvat evaluoinnin kohteeseen. Turvallisuustavoitteet voidaan määrittää esimerkiksi lakien tai muiden määräysten perusteella. Nämä tavoitteet on saavutettava hyvin määritellyillä turvallisuusominaisuuksilla. Jotta turvallisuusominaisuuksien oikeellisuus voidaan tutkia ja varmistaa, esitetään myös ne mekanismit, joilla toiminnallisuus saavutetaan.

Jokaiselle evaluointitasolle on lueteltu ne asiat, jotka sponsorin on toimitettava evaluoinin tekijälle. Sponsorin pitää huolehtia siitä, että nämä asiat toimitetaan tavalla, joka täytää asetetut vaatimukset ja että niiden perusteella voidaan todistaa se mitä tarvitaan.

Optimaalisessa tapauksessa evaluoinin tekijä on mukana jo tuotekehitysvaiheessa. Tällöin saavutetaan hyvä yhteisymmärrys evaluoijan ja sponsorin välillä. Se korostuu varsinkin korkeimmilla tasoilla, jossa kohde evaluoidaan hyvin tarkasti.

### 2.2.4. ITSEC:in F-C2 toiminnallisuus esimerkki

TCSEC määrittelee erilaisia evaluointiluokkia. Evaluointiluokat on nimetty kirjaimilla D:stä A:han. Mitä korkeammalla tasolla evaluointi on tehty, sitä enemmän sen oikeellisuuteen voidaan luottaa. Korkeampi evaluointitaso asettaa myös suuremmat turvallisuusvaatimukset tuotteelle. Kaikki evaluointitasot vaativat tietysti, että alemman tason vaatimukset täytetään. (Ylemmät tasot B1 - A1 mainitaan vain lyhyesti. Ne eivät kuulu tämän työn piiriin)

- D on minimaalisen turvallisuuden taso. TCSEC:ssä se on varattu järjestelmille, jotka evaluoidaan ja todetaan turvattomiksi. Tähän luokkaan kuuluisi esimerkiksi MS-DOS, jos joku sen päättäisi evaluoida.
- C1 - vapaa turvallisuustaso, käyttäjiä ei vaadita tunnistettaviksi. Esimerkiksi pelkkä käyttäjäryhmä on riittävän tarkka tunnistus.
- C2 - kontrolloituun pääsyyn perustuva turvallisuus. Objekteilla on oltava turvallisuusmäärittelyjä, käyttäjät on oltava tunnistettuna jne. Tämä käsitellään seuraavassa tarkemmin.
- B1 - Objekteilla on oltava määriteltynä erilaisia turvallisuustasoja (Labeled security protection). Turvallisuustasot voivat olla esimerkiksi julkinen, salainen, erittäinsalainen jne. Tietoa, mikä on julistettu salaiseksi ei esimerkiksi saa tulostaa kirjoittimella joka on julkinen. Prosessien eristäminen toisistaan.
- B2 - rakenneturvallisuus. (Structured protection). Kaikkia järjestelmän kohtia, joista siihen on mahdollista päästä käsiksi on auditoitava. Toisiin ohjelmiin kohdistuvat muistiviittaukset on estettävä jo laitteistotasolla. Järjestelmässä on oltava erillinen operaattori ja ylläpitäjä.
- B3 - Turvallisuusdomainit. Hälytykset turvallisuusrikkeistä (esim. summeri),Tarkat ja yksinkertaiset suojausmekanismit, jotka varmentavat toimintoja kuten:

kerroksellisuus, tiedon piilottaminen ja erilaiset abstraktiotasot. Kaikki tiedonsäilytys paikat pitää olla myös turvallisia ja valvottuja (varmuuskopiot jne.). Lisää vaatimuksia dokumentointiin ja testaukseen.

- A1 - Varmennettu suunnittelu Turvallisuustasoltaan samaa luokkaa kuin B3-taso, mutta suunnittelu, rakenneratkaisut ja testaus on oltava varmennettua. Kaikki mahdollinen on todistettava oikeaksi.

Toiminnalliset vaatimukset F-C2:lle perustuvat USA:n TCSEC:in C2:n vaatimuksiin. C1 verrattuna sillä saavutetaan tarkempi pääsynvalvonta, eli käyttäjien tekemisiä voidaan valvoa paremmin.

### *Tunnistus ja varmennus*

Kaikki käyttäjät on voitava tunnistaa ja varmentaa yksilöllisesti. Tunnistus ja varmennus on aina tehtävä ennenkuin käyttäjä voi tehdä mitään muuta. Varmennustieto on säilytettävä niin, että ainoastaan halutut käyttäjät voivat päästä siihen käsiksi. Jokaiselle tapahtumalle on pystyttävä määrittämään tekijä /s s123-125/.

## *Pääsynvalvonta*

Kohteen on pystytävä erottamaan ja määrittelemään jokaisen käyttäjän ja objektin väliset oikeudet. Oikeudet voidaan jakaa ylläpitäjän, käyttäjäryhmän tai käyttäjän oikeuksiin. Tarvittaessa haluttujen käyttäjien tai käyttäjäryhmien pääsy objekteihin on pystyttävä kieltämään. Lisäksi pitää olla mahdollista rajata käyttäjän oikeudet sellaisiksi, että käyttäjä pystyy käyttämään objektia, mutta ei pysty muuttamaan sitä. Jokaisen objektin oikeudet on voitava määritellä käyttäjätasolle asti. Käyttäjät, joilla ei ole oikeutta, eivät voi muuttaa objektin oikeuksia. Vastaavasti ainoastaan tietyt käyttäjät saavat lisätä tai poistaa käyttäjiä järjestelmästä.

Aina kun yritetään tehdä operaatiota, joka vaatii ylläpitäjän oikeuksia, pitää oikeudet varmentaa, ja mikäli niitä ei ole, operaatio on kiellettävä.

## *Seuranta*

Kohteen tulee sisältää seurantakomponentteja, jotka mahdollistavat seuraavien tapahtumien seuraamisen. Näistä tapahtumista muodostetaan loki, josta voidaan jälkeenpäin todeta mitä on tapahtunut. Seurattavia tapahtumia ovat:

- Tunnistus- ja varmennusmekanismien käyttö. Vaadittavat tiedot: päiväys, kellonaika, annettu käyttäjätunnus, tieto siitä, mistä yritys on tehty (esimerkiksi päätteen tunnus) ja lopputulos - onnistuiko tunnistus vai ei.

- Yritys käyttää objektia, mikä on pääsynvalvonnan alainen. Vaadittavat tiedot: päiväys ja kellonaika, käyttäjätunnus, objektin nimi, käytön tyyppi ja lopputulos.

- Yritys sellaisen objektin luomiseksi tai tuhoamiseksi, joka vaatii ylläpitäjän oikeuksia. Vaadittavat tiedot: päiväys, kellonaika, käyttäjätunnus, objektin nimi ja yritetty toimenpide.

- Varmennettujen käyttäjien toimenpiteet, jotka vaikuttavat kohteen turvallisuusasetuksiin. Vaadittavat tiedot: päiväys, kellonaika, käyttäjätunnus, operaation tyyppi (käyttäjien luominen ja poistaminen, tallennusmedian lisääminen tai poistaminen järjestelmästä, sekä järjestelmän käynnistäminen tai sammuttaminen)

### *Auditointi*

Tunnistamattomat käyttäjät eivät saa päästä käsiksi seurantatietoihin. Työkalut, joilla seurantatietoja käsitellään, tulee toimittaa ja olla dokumentoituina. Työkalujen tulee pystyä erittelemään yksittäisiä käyttäjiä tai käyttäjäryhmiä.

### *Resurssiobjektien uudelleenkäyttäminen*

Kaikki tiedonsäilytysobjektit, joita palautetaan järjestelmälle pitää tyhjentää ennenkuin ne annetaan seuraavalle käyttäjälle. Tämä tulee tapahtua niin että lopputuloksesta ei voida tehdä johtopäätöksistä siitä, mitä tietoa objektissa aikaisemmin oli.

# 3. Lähtökohta

Työn tavoitteena oli suunnitella ja toteuttaa turvallinen ja hallittu Windows ympäristö. Voidaksemme määritellä millainen ympäristön pitäisi olla, pitää ensin tarkastella Windowsin rakennetta ja toimintaa turvallisuuden ja konfiguraationhallinnan kannalta.

Microsoft Windowsia suuniteltaessa turvallisuusnäkökohdat eivät olleet mitenkään tärkeitä. Alunperin Windows oli vain graafinen käyttöliittymä DOS:lle. Sen tehtävänä oli mahdollistaa ohjelmien käynnistäminen graafisesta käyttöliittymästä ja antaa eri ohjelmille yhdenmukainen ilme. Windows oli siis eräänlainen graafinen kuori (shell). Windows saavutti kuitenkin uskomattoman suosion, ja sen käyttö levisi lähes kaikille aloille. Tällä hetkellä Windows on markkinoiden suosituin sovellusohjelmien toimintaympäristö.

DOS ei tarjoa riittäviä valmiuksia turvallisen järjestelmän rakentamiseen. DOS on käyttöjärjestelmänä liian pelkistetty. Turvallisuuden kannalta sen rakenne sisältää suuria aukkoja (muistinsuojaus, prosessien eristäminen, tietostojärjestelmän puutteet, autentikoinin puuttuminen jne.) Yleisessä tapauksessa DOS:n rakenteellisia puutteita on mahdotonta korjata ulkopuolisella ohjelmalla niin, että lopputuloksesta tulisi turvallinen. Jos halutaan yleiskäyttöinen turvallinen ympäristö, DOS:sta on pakko luopua, käyttäjärjestelmän puutteiden korjaamiseen tarvitaan toinen parempi käyttöjärjestelmä.

Koska DOS:sta, ja samalla Windowsista, luopuminen ei kuitenkaan ole mahdollista, pitää keksiä jokin toinen ratkaisu. Vaikka yleistä turvallista ratkaisua Windowsin turvallisuusongelmiin ei ole olemassa, on mahdollista rakentaa järjestely jossa alunperin turvattomasta DOS:sta ja sen päällä toimivasta Windowsista rakennetaan mahdollisimman turvallinen järjestelmä.

Seuraavassa käydään läpi Windows työasemaverkon rakennetta ja sen jälkeen tarkastellaan palvelimen ja Windows-työaseman ominaisuuksia turvallisuuden kannalta.

## 3.1. Työasemaverkko

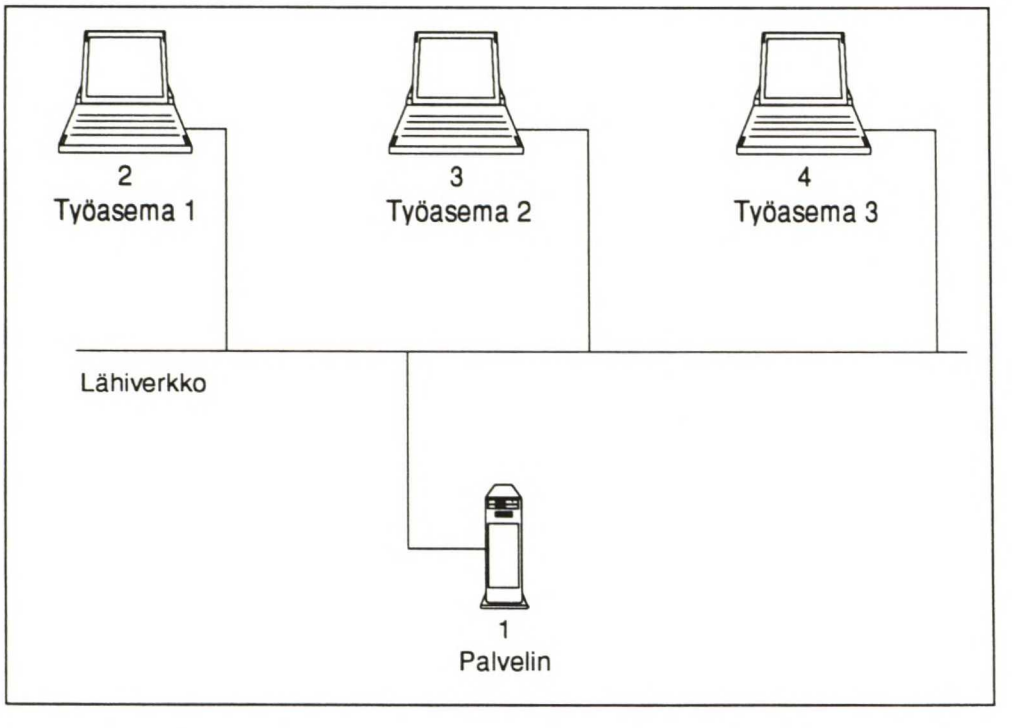
*Windows-työasemaverkolla tarkoitetaan järjestelmää, jossa useita työasemia ja yksi tai useampia palvelimia on kytketty toisiinsa lähiverkon kautta (kuva 1).*

Työasemat pystyvät jakamaan ja käyttämään toistensa resursseja, mutta useinmiten ne jakavat palvelimen resursseja. Ideana on se, että työasemat käyttävät samaa palvelinta ja näin saadaan helposti jaettua tietoa ja tehostettua resurssien käyttöä.

Palvelin on yleensä tavallista työasemaa tehokkaampi tietokone, jossa on paljon levytilaa ja johon on kytketty kirjoitin. Palvelimessa käytetään tavallisesti työasemaan verrattuna monipuolisempaa ja turvallisuuden kannalta parempaa käyttöjärjestelmää. Palvelimien käyttöjärjestelminä käytetään esimerkiksi Windows NT:tä, UNIX:a, OS/2:ta tai NetWare:a.

Työasemat ja palvelimet keskustelevat toistensa kanssa lähiverkon kautta. Yhteydet muodostetaan käyttäjäkohtaisesti, ja yleisesti käyttäjän on oltava palvelimelle tunnettu ennenkuin palvelimen käyttö on sallitua.

Lähiverkkona käytetään tavallisesti Ethernet:ä tai Token Ring:ä. Kumpaakaan edellä mainituista lähiverkoista ei voida pitää turvallisina, koska niiden liikennettä voidaan salakuunnella. Lähiverkon fyysinen suojaaminen ei kuitenkaan kuulu tämän työn piiriin.




Kuva 1.

## 3.2. Verkkokäyttöjärjestelmän ominaisuudet

Turvallisen järjestelmän rakentaminen tarvitsee ainakin yhden kohteen, jota voidaan pitää luotettavana. Windows-työasemaverkossa luotettavana osapuolena voidaan pitää verkon palvelinta. Tässä työssä palvelimen ja verkkokäyttöjärjestelmän oletetaan täyttävän turvakriteerit.

*Verkkokäyttöjärjestelmällä tarkoitetaan palvelinta ja sitä kokonaisuutta miten palvelin tarjoaa verkkoon palveluitaan. Verkkokäyttöjärjestelmä on joko sisäänrakennettu varsinaiseen palvelimen käyttöjärjestelmään tai se toimii omana palvelunaan käyttöjärjestelmän päällä.*

Palvelimessa käytettävät käyttöjärjestelmät ovat turvallisuusominaisuuksiltaan paljon parempia kuin pelkkä Windows ja niiden palveluiden käyttäminen vaatii sisäänkirjottautumisen palvelimelle.

Kaikki palvelimen käyttäjät ovat tunnettuja ja pystytään erottelemaan kuka on kuka. Myös palvelimen tiedostoilla on omistajat, ja niille voidaan asettaa tiedosto-oikeuksia. Tavallisesti käyttäjät eivät pysty lukemaan toistensa tiedostoja.

Palvelimen suojaaminen on tavallisesti paljon yksinkertaisempaa kuin työaseman suojaaminen, sillä palvelimessa on parempi käyttöjärjestelmä, jonka ohittaminen on monimutkaisempaa kuin Windows-työaseman.

Lisäksi palvelin voidaan helpommin suojata fyysisesti sijoittamalla se turvalliseen tilaan lukkojen taakse.

### 3.2.1. Microsoft Networking

Microsoft Networking käsittää erilaiset LAN Manager-sukuiset verkkoympäristöt. LAN Manager verkoissa puhutaan domain-käsitteestä.

*Domain on ryhmä palvelinkoneita jotka jakavat käyttäjä- ja ryhmätiedot.*

Domainilla on nimitettynä yksi palvelin, joka toimii tiedon jakajana; tätä kutsutaan domain-kontrolleriksi. Domain-kontrollerissa sijaitsee käyttäjätietokanta, ja tätä tietoa kopioidaan yksisuuntaisesti muihin domainin palvelimiin. Näitä muita palvelimia kutsutaan backup domain-kontrollereiksi. Kaikki käyttäjätietoja koskevat päivitykset on tehtävä aina domain-kontrolleriin.

Eri domainien välille pystytään luomaan niin sanottuja luotettuja suhteita (trusted domains).

*Luotetulla domainilla tarkoitetaan sitä että palvelin luottaa toisessa luotetussa domainissa tehtyihin käyttäjien validiointeihin.*

Luottamus on yksisuuntainen, jos halutaan luottamussuhde molempiin suuntiin, pitää se myös määritellä erikseen molempiin suuntiin. Luotettujen domainien välillä voidaan välitää globaaleja ryhmiä, joille voidaan asettaa pääsyoikeuksia.

Kun käyttäjä on autentikoituna domainiin, hän pystyy käyttämään kaikkia samassa domainissa olevia palvelimia ilman, että hänen täytyy erikseen sisäänkirjottautua niihin.

Palvelimesta jaetaan resursseja niin sanottuina jakoina (share). Jako on nimi, jolla työasemasta voidaan pyytää tiettyä resurssia. Resursseja ovat levyn tiedostohakemistot ja kirjoittimet.

LAN Manager verkkokäyttöjärjestelmät toimivat erilaisten käyttöjärjestelmien päällä. LAN Managerista on olemassa versiot IBM:n OS/2:lle ja erilaisille UNIX:eille. IBM on tehnyt oman LAN Manager yhteensopivan verkkokäyttöjärjestelmän nimeltään LAN Server.

NT-networking on uudempi versio LAN Manager-verkoista. NT on turvallisempi verkkokäyttöjärjestelmä kuin vanhempi LAN Manager, ja se vaatii myös hieman omaa käsittelyä. AT&T on rakentanut NT server konseptin myös UNIX-koneille. NT Advanced Server for UNIX toimii tällä hetkellä vain AT&T:n UNIX ympäristöissä, mutta on pian tulossa myös muille valmistajille.

## 3.2.2. Novell NetWare 3

Novell NetWare 3 oli Novell:in suuri menestys. Tälläkin hetkellä NetWare 3 on maailman eniten käytetty verkkokäyttöjärjestelmä. NetWaren ideana on rakentaa käyttöjärjestelmä, joka toimii pelkästään verkkopalvelimen käyttöjärjestelmänä. Verkkokäyttöjärjestelmän suorituskyky on optimoitu nimenomaan tiedostojen nopeaan välitykseen /5/.

NetWare 3:ssa palvelimet ovat erillään toisistaan, eivätkä ne ole toisistaan tietoisia. Jos käyttäjä haluaa käyttää useampia palvelimia, hänen pitää erikseen kirjottautua sisään niihin.

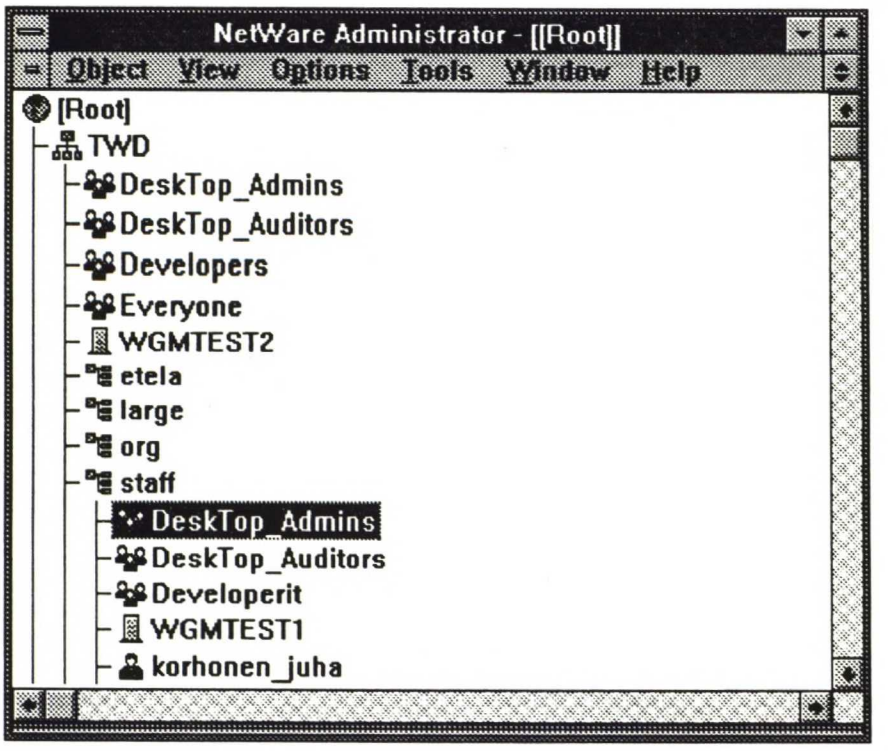
## 3.2.3. Novell NetWare 4

NetWare 4:ssa Novell halusi tarjota menetelmän, jolla eri palvelimet olisivat tietoisia toisistaan, ja käyttäjän tarvitsisi kirjottautua sisään järjestelmään vain kerran. NetWare 4:ssä on käytössä niin kutsuttu NetWare Directory Services-järjestelmä (NDS), jossa työasemaverkko muodostaa puumaisen hierarkian, johon kaikki verkon palvelimet on kytketty.

Hierarkiaa voidaan rakentaa eri tavoilla. Se voi perustua esimerkiksi yrityksen toiminnalliseen hierarkiaan tai maantieteelliseen sijaintiin. Puu voi siis olla maantieteellisesti hyvin laaja. (Kuva 2.)

### *Nimeämiskäytäntö*

Puuhun on liitetty objekteja joilla on oma yksiselitteinen nimi. Nimi kootaan samaan tapaan hierarkisesti kuin X.400 nimeämiskäytännössä /6/. Esimerkiksi käyttäjä, joka sijatsee Helsingin toimipisteen testausyksikössä voi olla määritelty: cn=käyttäjänimi.ou=testing.o=Helsinki. Vastaavasti testausryhmän palvelin voisi olla nimeltään: cn=palvelin.ou=testing.o=Helsinki. (cn = common name, ou = organization unit, o=organization)




Kuva 2

# 3.3. Työaseman ominaisuudet

## *Windows ja DOS*

Windows ei ole itsenäinen käyttöjärjestelmä, vaan se vaatii toimiakseen DOS:n.

*Tässä työssä Windows-käyttöjärjestelmällä tarkoitetaan DOS:n ja Windowsin yhdistelmää.*

DOS on hyvin pelkistetty ja minimaalinen käyttöjärjestelmä. DOS ympäristössä käyttäjällä on mahdollista suorittaa kerrallaan vain yhtä ohjelmaa. Ohjelma saa käyttöönsä koko tietokoneen ja sillä on täysi vapaus tehdä mitä se haluaa. Hyvänä puolena on, että ohjelma pystyy periaatteessa saamaan maksimaalisen tehon irti tietokoneesta, koska prosessori aikaa ei tarvitse jakaa muiden prosessien kesken. Käytännössä tilanne on kuitenkin hieman toinen. Tänä päivänä käyttöjärjestelmän perusvaatimuksiin kuuluu se, että tietokoneella on mahdollista suorittaa useita samanaikaisia ohjelmia. DOS sisältää joitakin rajoituksia, joista tunnetuin on 640 kilotavun maksimikoko ajettavalle ohjelmalle. Tätä rajoitusta pyritään kiertämään erilaisilla muistiajureilla, jotka mahdollistavat suurempien muistialueiden käytön. DOS käyttää segmentoitua muistimallia, jossa segmentin koko on 64 kilotavua. Suurin yhtenäinen muistialue, joka pystytään varaamaan on siis 64 kilotavua.

Windows toimii DOS:n päällä ja tästä johtuu se, että DOS:n rajoitukset koskevat myös Windowsia. Windowsin suosion kasvaessa ja tietokonelaitteistojen parantuessa DOS:n rajoitukset alkoivat kuitenkin häiritä yhä enemmän, ja Windows joutui ottamaan haltuunsa tehtäviä, joita DOS ei osannut tehdä tai teki liian hitaasti tai huonosti. Vähitellen Windows sai yhä enemmän käyttöjärjestelmälle kuuluvia tehtäviä. Windows huolehtii muun muassa virtuaalimuistista, tiedostonkäsittelystä (32-bittinen tiedostojenkäsittely), ja Windowsissa on käytössä myös yhteistoimintainen moniajo (ns. co-operative multitasking). Ohjelmat toimivat samanaikaisesti, mutta sovellusohjelmilla on velvollisuus antaa toiminta-aikaa toisilleen. Huono puoli on se, että huonosti käytäytyvä sovellus voi varata koko koneen ja kaikki muut sovellukset joutuvat odottamaan.

## *Autentikointi*

Autentikoinnilla tarkoitetaan, että käyttäjän pitää kertoa käyttöjärjestelmälle kuka hän on. Käyttäjän kertoma käyttäjätunnus on myös varmennettava jollakin tavalla, tavallisesti se tehdään kysymällä käyttäjältä salasana. Tällöin käyttäjän on oltava ennalta esitelty

käyttöjärjestelmälle. Esittelyn tekee tavallisesti järjestelmän ylläpitäjä. Jos käyttäjää ei ole olemassa tai annettu salasana ei ole oikea, tietokonetta ei pääse käyttämään.

*Autentikointi määritellään tässä yhteydessä tarkoittamaan käyttäjän tunnistamista ja tunnistuksen varmentamista.*

Windowsista puuttuu käyttäjän pakollinen autentikointi. Jos tietokoneella on vain yksi käyttäjä voidaan autentikointi tietysti hoitaa vaikka käynnistys-salasanalla; jotta tietokone voidaan käynnistää, kysytään salasana. Jos tietokoneella on useampia käyttäjiä, ongelmana on, että kaikki joutuvat käyttämään samaa salasanaa. Jos joku muuttaa salasanan, niin muut eivät enää pääse käyttämään konetta.

Tietoturvallisuuden kannalta autentikoinnin puuttuminen Windowsissa on paha puute, koska ei tiedetä kuka käyttäjä on. Jos sisäänkirjottautuminen tehdään, se tehdään ainoastaan verkkokäyttöjärjestelmään. Tämä suojelee ainoastaan palvelimen resursseja, eikä vaikuta lainkaan paikallisen Windows-työaseman käyttöön. Käyttäjän ei ole edes pakko kirjottautua sisään verkkoon. Paikalliseen Windowsiin uusi käyttäjä luodaan automaattisesti jos häntä ei ole olemassa. Kukaan ei siis kontrolloi sitä, kuka saa käyttää konetta.

Jos käyttäjä ei ole tunnettu, on mahdotonta tehdä käyttäjäkohtaisia turvallisuusasetuksia.

Koska kaikki käyttäjät ovat samanarvoisia, ei ole olemassa erillistä ylläpitäjää - kaikki koneen käyttäjät toimivat myös ylläpitäjinä. Windowsissa ei voida estää käyttäjää tekemästä muutoksia järjestelmään. Halutessaan kaikki käyttäjät pystyvät esimerkiksi alustamaan kaikki työaseman levyt tai lukemaan muiden samaa konetta käyttävien henkilöiden salaamattomia tiedostoja.

### *Muistinsuojaus*

Windowsissa ei ole muistinsuojausta. Hyvän käyttöjärjestelmän tehtäviin kuuluu eri prosessien ja objektien erottaminen toisistaan niin, että ne eivät voi käsitellä toistensa muistialueita /3/. Windowsissa muistinsuojauksen puuttumisesta aiheutuu tietoturvaongelmia. Halutessaan sovellusohjelmat (esim. virukset) voivat käydä läpi toisten sovellusten muistia ja etsiä niistä tietoa.

*Muistinsuojauksella tarkoitetaan sitä että eri ohjelmien muistiavaruudet ovat erotettuja toisistaan, eivätkä ne pysty viittaamaan toistansa muistiavaruuksiin.*

Windowsissa on myös mahdollisuus koukuttaa käyttöjärjestelmän tai muiden kirjastofunktioiden kutsumista.

*Koukutus (hooking) on toimenpide, jossa kutsuttaessa jotakin funktiota, kutsutaankin ennen varsinaisen systeemifunktion kutsumista ns. koukutusfunktiota, joka voi tehdä haluamiaan toimenpiteitä ennen varsinaisen funktion kutsumista.*

Turvallisuusongelma aiheutuu esimerkiksi kun sovellusohjelma kutsuu vaikkapa salasanan vaihtofunktiota, tapahtuukin niin, että ensin kutsutaan toista ns. koukkufunktiota ja vasta sen jälkeen kutsutaan varsinaista salasanan vaihtofunktiota. Tietoturvasta ei voida juuri voida puhua, jos mahdollinen uhkaaja saa oman ohjelmansa käynnistettyä Windowsissa, koska kaikki käyttöjärjestelmän palvelut ja kaikkien sovellusten toiminta voidaan näin kaapata.

### *Tiedostojärjestelmä*

Windowsilla ei ole omaa tiedostojärjestelmää vaan se käyttää DOS:n FAT-tiedostojärjestelmää /4/. Tietoturvan kannalta tämä on ongelmallista, koska kaikkiin Windowsin tiedostoihin pääsee käsiksi jo ennen Windowsin käynnistymistä. FAT on varsin yksinkertainen ja samalla haavoittuvainen tiedostojärjestelmä. Tiedostoilla ei ole omistajaa eikä luojaa, vaan ne ovat samanarvoisia. Tiedostoilla voi tosin olla erilaisia attribuutteja. Attribuutteja ovat: "read-only", "system" ja "hidden". "Read-only" tarkoittaa vain lukuoikeutta, tiedoston päälle ei voi kirjoittaa sitä voidaan vain lukea. "System"-attribuutilla merkitään käyttöjärjestelmän tiedostoja. "Hidden"-attribuutilla merkittyjä tiedostoja ei normaalisti näytetä hakemistolistoissa. Kaikki käyttäjät tosin voivat muuttaa tiedoston attribuutteja. Koska Windowsin käyttäminen ei vaadi käyttäjän tunnistamista, ei myöskään tiedostoille voi asettaa oikeuksia. Kaikki käyttäjät ovat keskenään samanarvoisia, joten kuka tahansa joka pääsee koneeseen käsiksi voi muuttaa mitä haluaa. Kaikki tieto, joka on salaamattomana tietokoneen kovalevyllä, on julkisesti luettavissa.

## *Windowsin hakemistorakenne*

Kun Windows asennetaan tietokoneeseen, käyttäjä kertoo mihin hakemistoon Windows asennetaan. Tästä hakemistosta tulee Windowsin päähakemisto. Päähakemistoon asennetaan Windowsin mukana tulevat ohjelmat, sinne laitetaan kaikki ohje-tiedostot ja siellä säilytetään Windowsin konfiguraatiotietoja.

*Windowsin päähakemisto on se hakemisto johon Windows on asennettu.*

Päähakemiston alapuolelle tehdään system-hakemisto, jossa puolestaan säilytetään Windowsin itsensä käyttämät ohjelmatiedostot, erilaiset ajurit, kirjasinlajit ja käyttöjärjestelmän jaetut kirjastot eli ns. DLL-tiedostot. (DLL - dynamically linked library). Jaetun kirjaston ideana on, että useampi ohjelma voi tarvittaessa käyttää sitä samanaikaisesti - ohjelmat siis jakavat sen. Lisäksi jaettua kirjastoa tarvitaan muistissa vain yksi kappale, riippumatta siitä montako ohjelmaa käyttää sitä.

## *Windowsin konfiguraatiotiedostojen rakenne*

*Windowsin konfiguraatiotiedot määrittelevät mitä laitteistoja työasemaan on asennettu ja miten Windows toimii.*

Windowsin konfiguraatiotiedot säilytetään pääasiassa tekstimuotoisissa konfiguraatio-tiedostoissa. Näillä tiedostoilla on yleensä nimen loppupäätteenä .ini, joten niitä kutsuttaankin usein ini-tiedostoiksi.

*Ini-tiedosto on tekstimuotoinen konfiguraatiotietoa sisältävä tiedosto. Sen rakenne on määritelty. Ini-tiedosto jakautuu osioihin (section), joissa on tekstimuotoisia rivejä, joilla kullakin on avain ja arvo.*

Windows tarjoaa funktiot näiden ini-tiedostojen käsittelyyn. Ini-tiedoston maksimi koko on 64 kilotavua. Tästä kokorajoituksesta aiheutuu myös ongelmia, koska tiedoston koon kasvaa yli tämän rajan, sitä ei pystytä enää käsittelemään kunnolla. Toinen ini-tiedostojen ongelma on, että niiden käsittely hidastuu mikäli niiden koko kasvaa. Jos Windowsia käynnistettäessä joudutaan käymään läpi paljon isoja ini-tiedostoja, kestää sen käynnistyminen kauan.

Ini-tiedostoja on monenlaisia. System.ini sisältää systeemin määrittelyjä: mitä ajureita ladataan Windowsin käynnistyessä, mikä ohjaa hiirtä, millainen lähiverkko on asennettuna, näppäimistön- ja näyttökorttin tiedot, yms. Win.ini sisältää erilaisten Windows-ohjelmien asetuksia, tietoja eri kirjasinlajeista ja ikkunoiden paikoista. Ini-tiedostoja on kymmeniä erilaisia, esimerkiksi kirjoittajan tietokoneessa on 126 erilaista ini-tiedostoa. Kuvassa 3. on esitettynä tyypillinen asetustiedoston osio. Siinä on esitetty asetukset Logitech:n hiirtä varten. Hiiren tyyppi on sarja-hiiri, sen malli on "Mouseman", se on kytketty sarjaporttiin com1 ja "DragLock" ei ole päällä.

```
[LogiMouse]
Type=Serial
Model=MouseMan
Port=1
DragLock=None
```

Kuva 3.

Erilaisilla sovellusohjelmilla on myös omia ini-tiedostojaan. Ini-tiedostot voivat sijaita joko Windows-hakemistossa tai siinä hakemistossa, johon sovellus on asennettuna.

Koska ini-tiedostot ovat tekstimuotoisia, niiden lukeminen ja muuttaminen on helppoa. Ongelmana on vain se, että yleensä ei tiedetä mitä mikin asetus tekee tai mihin se vaikuttaa. Joidenkin ohjelmien ohjekirjoissa on selitettynä kyseisen ohjelman käyttämät määrittelyt, mutta useinmiten mitään tietoa ei ole saatavilla. Konfiguraatiotietoja muutetaan ja tutkitaan yleensä sovellusohjelmalla, joka esittää tiedon ihmiselle helpommin ymmärrättävässä muodossa.

### *Program Manager*

Program Manager on varmasti Windowsin tunnetuin ohjelma. Sen tehtävä on toimia Windowsin kuorena (eli shellinä). Kuoren tehtävänä taas on toimia käyttöjärjestelmän ja käyttäjän välissä. Se käynnistää käyttäjän haluamia ohjelmia ja esittää käyttäjälle mitä on käytettävissä.

Kun shellinä toiminut ohjelma sammutetaan, samalla sammutetaan myös koko Windows ja työasema palaa DOS:in.

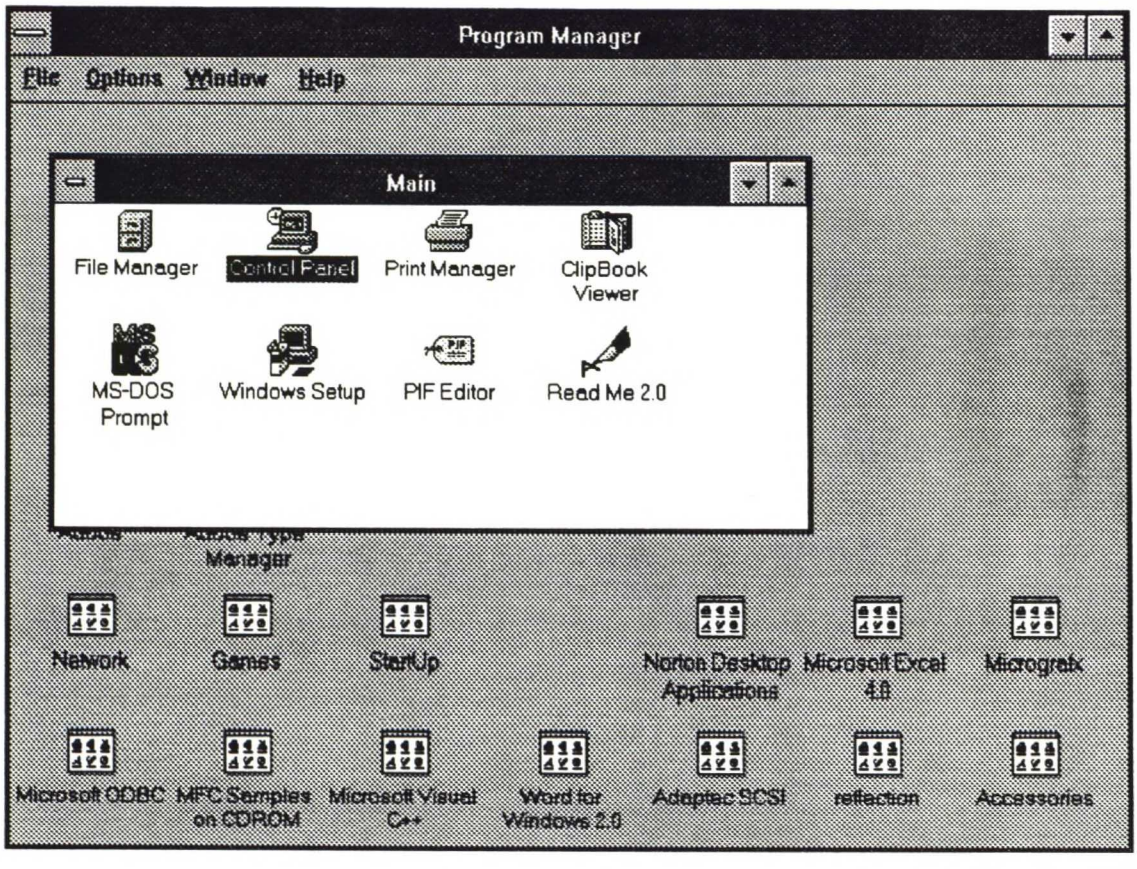
Program Manager käynnistyy tavallisesti aina kun Windows on käynnistetty. Se esittää ikoneina käytettävissä olevat ohjelmat, jotka voi käynnistää klikkaamalla hiirellä ko. ikonia (Kuva 4).

Periaatteessa shellinä voi toimia mikä tahansa ohjelma, vaikkapa tekstinkäsittelyohjelma, mutta tällöin tietokoneen käyttömahdollisuudet ovat rajoitetut. Käyttäjä ei yksinkertaisesti pysty käyttämään mitään muuta kuin tekstinkäsittelyohjelmaa, ja uusien ohjelmien käynnistäminen on mahdotonta. Tietyissä tilanteissa tämä voi olla myös toivottavaa, esimerkiksi jos tietokone toimii pankin kassana, ja siinä ajetaan vain kassasovellusta.

Program Managerin lisäksi Windowsin mukana tulee myös toinen shellinä toimiva ohjelma nimeltään File Manager. Sitä käytetään tavallisesti tiedostojärjestelmän

tutkimiseen ja käyttämiseen. File Manager on tarkoitettu tiedostojen kopioimiseen ja siirtämiseen, mutta siitä voidaan yhtä hyvin käynnistää ohjelmia.

Program Managerilla on myös oma konfiguraatiotiedostonsa josta voidaan konfiguroida sen käyttäytymistä.




Program Manager (Kuva 4)

Program Managerissa ohjelmia ja dokumentteja esitetään käyttäjille pieninä kuvina, *ikoneina* (kuva 4). Ohjelma ikoneista on koottu ryhmiä. Näitä ryhmiä kutsutaan *ohjelmaryhmiksi*.

Ohjelmaryhmien sisältöä ja sijaintia säilytetään erillisissä *grp-tiedostoissa*, mitkä sijaitsevat Windows-hakemistossa. Jos samalla työasemalla on useita käyttäjiä, joutuvat kaikki käyttäjät jakamaan samat ohjelmaryhmät.

# 4. Työn tavoite

Tämän työn tarkoituksena oli kartoittaa Microsoft Windowsin turvallisuus ja konfiguraationhallinnan puutteita ja toteuttaa ympäristö, jossa Windowsia voidaan käyttää turvallisesti.

Turvallisuuden tavoitteeksi asetettiin ITSEC:in FC-2:den turvallisuusvaatimukset.

FC-2 toiminnallisesta määrittelystä saadaan perusta, jonka päälle voidaan alkaa kokoamaan turvallista Windows-järjestelmää. FC-2 ei kuitenkaan määrittele turvallisuuden toteuttamistapoja, vaan kertoo yleisellä tasolla mitkä asiat ovat turvallisuuden kannalta tärkeitä, ja mihin yksityiskohtiin on kiinnitettävä huomiota. Turvallinen Windows-ympäristö sisältää omia erityisvaatimuksiaan, ja nämä vaatimukset on huomioitava.

Pahimmat turvallisuusaukot Windowsissa, johtuvat käyttöjärjestelmän puutteista. Osa näistä puutteista on mahdollista korjata muilla ohjelmakomponenteilla, mutta syvällä käyttöjärjestelmän sisällä olevia puutteita on lähes mahdotonta korjata käyttöjärjestelmän ulkopuolelta. Tämä tekee yleisen ratkaisun tekemisen mahdottomaksi. Yleinen ratkaisu vaatii toisen käyttöjärjestelmän. Lähtökohtana oli kuitenkin se että pitää rakentaa turvallinen Windows-ympäristö, turvallisuus on siis pyrittävä rakentamaan jotenkin muuten.

Turvallisuustavoitteet voidaan saavuttaa etsimällä kaikki turvallisuuden kannalta ongelmalliset kohdat, ja suunnittelemalla järjestely, jossa käyttäjien oikeuksia rajoittamalla turvallisuuden ohittaminen tehdään mahdottomaksi. Käyttäjille oikeuksien rajoittamisesta aiheutuvat haitat on pyrittävä minimoimaan. Myös turvallinen Windows pitää olla mahdollisimman helppokäyttöinen.

Turvallisuuden lisäksi toisena tavoitteena oli hallittavan ympäristön tekeminen. Hallittavalla ympäristöllä tässä yhteydessä tarkoitetaan sitä, että Windows työasemaverkkon eri työasemia on voitava hallita keskitetysti.

Toteutettavan konfiguraationhallinnan tavoitteet ovat:

- Keskitetty ylläpito. Yhdestä työasemasta voidaan ylläpitää muita työasemia.
- Työasema on voitava jakaa usean käyttäjän kesken. Yhdellä työasemalla voi olla useampia kuin yksi käyttäjä. Käyttäjillä pitää voida olla henkilökohtaiset ympäristöt.

- Saman käyttäjän siirtyessä tietokoneelta toiselle, tarvittaessa hänen henkilökohtainen ympäristönsä pitää siirtyä mukana.

- Ohjelmia on pystyttävä asentamaan automaattisesti. Uudet ohjelmistot ja ohjelmistojen päivitykset on pystyttävä tekemään automaattisesti ja keskitetysti. Ohjelmistojen tarvitsemat konfiguraation muutokset on myös voitava tehdä keskitetysti ja automaattisesti.

### 4.0.1. Turvallisuuden evaluointi

Evaluointiprosessi vie paljon aikaa ja on kallis toteuttaa. Lisäksi evaluoinnit tyypillisesti koskevat vain tiettyä tietokonemallia, jolla evaluointi on tehty. Jos halutaan voimassa-oleva evaluointi tietylle tietokonemallille, joudutaan evaluointi tekemään erikseen. DeskTop:n kanssa päätettiin, että C2-evaluointia ei tässä vaiheessa tehdä. Jos joku asiakas sitä vaatii ja se katsotaan tarpeelliseksi, se tehdään myöhemmin.

Turvallisuutta on pyritty testaamaan yrittämällä itse kiertää turvallisuusasetuksia. Turvallisuuden kannalta kriittisiin kohtiin ohjelmistoa on yritetty kiinnittää erityistä huomiota. (Esimerkiksi jos salasanoja joudutaan kopioimaan tilapäispuskureihin, nämä puskurit tyhjennetään välittömästi käytön jälkeen.)

## 4.1. Toimintaympäristö

Aikaisemmin todettiin että turvallisuusvaatimusten saavuttaminen vaatii käyttäjien oikeuksien rajoittamista ja kieltämistä. Yleisessä tapauksessa oikeuksien rajoittamisella ei saavuteta aukotonta turvallisuutta, mutta useimmissa tapauksissa haluttu toiminnallisuus on mahdollista saavuttaa tietyin rajoituksin.

Rajoituksia aiheutuu siitä, että on pystyttävä kontrolloimaan mitä ohjelmistoja käyttäjät pystyvät käyttämään. Lähes tulkoon kaikki ohjelmistot saadaa toimimaan turvallisesti Windowsissa. Poikkeukset muodostavat kääntäjät ja tulkit - ohjelmat joilla on mahdollista tehdä käyttöjärjestelmäkutsuja, ja sitä kautta ohittaa järjestelmän turvallisuusominaisuudet.

Turvallisuus voidaan saavuttaa näin ollen toiminnoiltaan rajoitetussa käyttöympäristössä. Ylläpitäjien pitää pystyä luettelemaan sovellusohjelmat jotka ovat käyttäjien käytettävissä. Tavallisessa toimistoympäristössä, jossa tietokonetta käytetään pääasiassa erilaisten dokumenttien tuottamiseen, tai jonkun tietyn sovelluksen ajamiseen (esim. pääte pankin keskustietokoneeseen) tämä lähestymistapa toimii hyvin.

*Käyttäjien käytössä olevat ohjelmat ovat siis kiinteästi sidotut. He eivät saa pystyä tuomaan järjestelmään uusia ohjelmia, ilman että ylläpitäjät asentavat niitä heidän käyttöönsä.*

Käytännössä ylläpitäjä ottaa selville, mitä ohjelmistoja käyttäjät tarvitsevat ja haluavat käyttää. Ohjelmat asennetaan tietokoneeseen ja samalla tiedosto-oikeudet asetetaan siten, että käyttäjät pystyvät käynnistämään ohjelman, mutta eivät pysty vaihtamaan sitä. Samalla on varmistettava, että käyttäjät eivät pysty käynnistämään ohjelmia levykkeeltä, ja että esimerkiksi sähköpostitse käyttäjälle lähetettyä ohjelmaa ei pystytä suorittamaan. Tämä toiminnallisuus on mahdollista saavuttaa siten, että vain tietyissä hakemistoissa olevilla ohjelmilla on suoritusoikeudet, ja kaikkialla muualla olevilla ohjelmilla suoritusoikeutta ei ole.

Ohjelmien käyttöä on rajoitettu, sen sijaan tietoa sisältävät dokumentit eivät muodosta turvallisuuden kannalta ongelmaa.

Turvallinen järjestelmä vaatii, että käyttäjiä pystytään luokittelemaan erilaisiin ryhmiin, ei ole mahdollista, että turvallisessa järjestelmässä kaikki käyttäjät toimivat ylläpitäjinä. Turvallisuus vaatii ainakin kahden eri ryhmän erottamista toisistaan: ylläpitäjät ja käyttäjät.

### 4.1.1. Turvallisuus ennen Windowsin käynnistymistä

#### *Tietokoneen käynnistäminen*

Jos halutaan rakentaa turvallisempi Windows ympäristö on ensiksi varmistuttava siitä, että turvallisuutta ei voida ohittaa Windowsin ulkopuolelta. On turhaa puhua Windowsin turvallisuusominaisuuksista jos ne pystytään kiertämään vain olemalla käyttämättä Windowsia.

#### *BIOS*

Jos tietokoneen pystyy käynnistämään levykkeeltä, on lähes kaikki käyttöjärjestelmät ohitettavissa. Tästä syystä on pystyttävä estämään koneen levykkeeltä käynnistäminen. Useimmissa uusissa PC-tietokoneissa on mahdollista estää korpulta käynnistäminen tai laittaa käynnistysjärjestys sellaiseksi, että käynnistyminen tapahtuu ensin kovalevyltä. Tämä asetus tehdään koneen BIOS:lla. BIOS on tietokoneen emolevyllä ROM:ssa kiinteästi oleva ohjelma, joka huolehtii virran kytkemisen jälkeen koneen käynnistymisestä. BIOS on myös pystyttävä suojaamaan. Useissa BIOS:ssa voidaan asettaa salasana, joka vaaditaan ennenkuin BIOS:ksen asetuksia päästään muuttamaan. BIOS voidaan lisäksi palauttaa alkutilaan. Tämä tehdään esimerkiksi avaamalla tietokone ja irroittamalla akku siten että BIOS:n muisti tyhjenee. Alkutilaan palauttaminen voidaan estää vain lukitsemalla tietokoneen kotelo siten, että sitä ei saada auki. Kotelo on hyvä pitää suojattuna joka tapauksessa, koska muuten tietokoneesta voidaan vaihtaa tai varastaa sen massamuisti.

#### *Windowsin automaattinen käynnistäminen*

Windows työaseman käynnistyessä se käynnistyy ensin DOS:in. Tässä vaiheessa on pystyttävä pitämään huolta siitä, että Windows aina käynnistetään suoraan, eikä käyttäjä pääse keskeyttämään Windowsin käynnistymistä. Kun DOS käynnistyy, se suorittaa autoexec.bat nimistä komentotiedostoa. Autoexec.bat käynnistää tarvittavia muistinvaraisohjelmia ja asettaa ympäristömuuttujia. Jos autoexec.bat:issa on Windowsin käynnistyskomento, käynnistetään myös Windows automaattisesti. Ongelmana on kuitenkin se, että autoexec.bat:in suoritus voidaan keskeyttää control-c merkillä. Joissakin uusissa BIOS:ssa on mahdollista estää tämä (eräät Ami-winbios versiot), mutta tavallisesti käyttäjä voi kirjoittaa mitä haluaa. Jotta tätä voitaisiin estää, pitää ensimmäisenä operaationa käynnistää jokin ajuri, joka ottaa näppäimistön hallintaansa ja estää käyttäjää keskeyttämästä autoexec.bat:in suoritusta.

## 4.1.2. Turvallisuus Windowsin käynnistymisen jälkeen

### *Käyttäjienhallinta*

Kun Windows käynnistyy, on estettävä koneen käyttäminen ilman autentikointia. Se voidaan tehdä vaatimalla, että käyttäjän on kirjoitauduttava sisään (logon) verkkokäyttöjärjestelmään tai mikäli tietokone ei ole kytketty verkkoon toteutettava paikallinen sisäänkirjottautuminen työasemaan. Jos käyttäjä ei pysty kirjottautumaan sisään, ei hän myöskään pääse käyttämään tietokonetta.

*Sisäänkirjottautuminen on prosessi missä käyttäjä tunnistetaan (autentikoidaan) ja varmennetaan palvelimelle. Turvallisuus vaatii sisäänkirjottautumista aina ennenkuin käyttäjä voi käyttää tietokonetta.*

Verkkokäyttöjärjestelmissä uusia käyttäjiä pystyvät luomaan vain käyttäjät, joilla on ylläpitäjän oikeudet. Jos Windows-työasema ei ole kytketty verkkokäyttöjärjestelmään, joudutaan rakentamaan Windowsiin jokin systeemi, jolla käyttäjienhallinta tehdään. Jos palvelin on käytettävissä, Windows-työaseman ylläpitäjinä voidaan käyttää niitä käyttäjiä, jotka ovat myös verkkokäyttöjärjestelmän ylläpitäjiä.

*Ylläpitäjä on käyttäjä, jolla on oikeus tehdä muutoksia järjestelmässä. Turvallisessa järjestelmässä on kiinnitettävä erityistä huomiota niiden muutosten tekemiseen, jotka muuttavat turvallisuusominaisuuksia.*

Käyttäjätasojen (käyttäjä tai ylläpitäjä) lisäksi vaaditaan, että käyttäjien pitää olla järjestelmälle tunnettuja. Huolehditaan siitä, että käyttäjät poistuvat järjestelmästä, kun he ovat lopettaneet työskentelyn. Jos halutaan varmistaa, että käyttäjä ei vahingossa unohda itseään sisälle Windowsiin ja esimerkiksi poistu paikalta, voidaan Windowsin näytönsäästäjä suojata salasanalla ja asettaa tulemaan päälle tietyn ajan päästä. Jotta näytönsäästäjä voidaan poistaa, pitää käyttäjän antaa salasanansa uudestaan.

Käyttäjien tunnistamiseen liittyy oleellisena osana erilaisten oikeustasojen toteuttaminen. On pystyttävä erottelemaan käyttäjät joilla on oikeus tehdä turvallisuuteen vaikuttavia muutoksia tavallisista käyttäjistä. Jos kaikki käyttäjät pystyvät muuttamaan turvallisuusasetuksia, voivat he helposti kiertää turvallisuusvaatimukset.

### *Tiedosto-oikeudet*

Nyt kaikki käyttäjät ovat tunnettuja, mutta kaikilla on edelleen oikeus muuttaa mitä vain he haluavat. Käyttäjien oikeuksien rajoittamiseksi on rakennettava jonkinlaiset tiedosto-

oikeudet. Windowsissa on mahdollista koukuttaa kaikki funktiot, jotka käsittelevät tiedostoja.

Koukuttamalla kaikki mahdolliset tavat, joilla ohjelmat voivat käsitellä tiedostoja, voidaan rakentaa tiedosto-oikeudet Windowsiin.

Tiedosto-oikeuksilla on pystyttävä säätelemään kuka saa muuttaa konfigurointi-tiedostoja, sekä estämään tiedostojen tuhoaminen, ja toisten käyttäjien tiedostojen käsitteleminen. Olisi hyvä, jos tiedostoille voisi asettaa käyttäjäkohtaisia luku-, kirjoitus-, suoritus- ja tuhoamisoikeuksia.

### *Muistinsuojaus*

Windowsin muistinsuojauksen puuttumisen korjaaminen on jo paljon hankalampaa. Koska muistinsuojaus puuttuu, voivat käyttäjät rakentaa ohjelmia, joilla he voivat lukea toisten sovellusten muistia tai tehdä ohjelmia, jotka myös koukuttavat käyttöjärjestelmän palveluita tai jopa sitä suojaavaa ohjelmaa.

Muistinsuojaus on tavallisesti toteutettu varsin syvällä käyttöjärjestelmässä, ja myös Windowsissa se pitäisi rakentaa syvälle käyttöjärjestelmään. Tätä on hyvin vaikea toteuttaa käyttöjärjestelmän päälle.

Koska ei pystytä toteuttamaan varsinaista muistinsuojausta, tarvitaan siis jokin toinen tapa, jolla voidaan saavuttaa vastaava toiminnallisuus. Se voidaan saavuttaa, jos pystytään jotenkin rajoittamaan mitä ohjelmia käyttäjät voivat käynnistää tai asentaa Windowsiin. Tämä toiminnallisuus voidaan saavuttaa tiedosto-oikeuksien kautta. Tarvitaan hakemisto tai hakemistoja missä sijaitsevat kaikki ohjelmat, joita käyttäjä saa käynnistää, muut ohjelmat eivät käynnisty. Samalla on estettävä käyttäjää siirtämästä tiedostoja näihin hakemistoihin. Järjestely rajoittaa varsin paljon sitä, mitä käyttäjä voi ominpäin tehdä ja vaatii, että järjetelmän ylläpitäjä huolehtii kaikista tarvittavien uusien ohjelmien asentamisesta.

## 4.1.3. Turvallisuus Windowsin sulkemisen jälkeen

Käyttäjän lopetetttua työskentelynsä Windowsilla on pidettävä huolta siitä, että käyttäjä ei pääse palaamaan takaisin DOS:iin. Windowsin sulkemisen jälkeen on aina palattava hallitusti takaisin alkutilaan. Alkutila voi olla joko paluu takaisin kysymään uutta käyttäjätunnusta, tai tietokoneen sammuttaminen.

## 4.2. Konfiguraatio

Windowsin konfiguraatiolla tarkoitetaan kaikkia niitä asetuksia, jotka ovat voimassa käytetyssä tietokoneessa. Asetukset puolestaan määrittelevät sen miten Windows toimii, mitä se tarvitsee toimiakseen, mikä on sen toimintaympäristö, mitä eri ohjelmia on asennettuna ja miten ne toimivat. Konfiguraatio on siis hyvin tärkeä ja olennainen osa Windowsia.

*Tässä yhteydessä Windowsin konfiguraatiolla tarkoitetaan kaikkia niitä asetuksia, jotka määrittelevät Windowsin toiminnan.*

Konfiguraationhallintaa tarvitaan hallitun ympäristön muodostamiseen. Sillä voidaan toteuttaa käyttäjien ympäristöjen huomaamaton siirtäminen työasemasta toiseen ja saman Windows-työaseman jakaminen usean käyttäjän kesken niin, että kaikilla voi olla erilaisia asetuksia. Keskitetyllä konfiguraationhallinnalla voidaan helpottaa ylläpitäjien työtä ja samalla lisätä työasemien toimintavarmuutta, kun konfiguraatiot pysyvät paremmin kohdallaan.

Windowsin konfiguraatio voidaan selkeästi jakaa:

- Laitteistosta riippuvat asetukset. Asetukset, jotka ovat riippuvaisia siitä laitteisto kokoonpanosta mikä työasemassa on, ovat sille työasema kuuluvia asetuksia. Näiden asetusten siirtäminen työasemasta toiseen ei ole mahdollista, sillä ne todennäköisesti eivät toimi toisessa ympäristössä.

- Laitteistosta riippumattomat asetukset ovat puolestaan siirrettäviä. Näitä asetuksia on mahdollista kopioida työasemasta toiseen ilman, että siitä aiheutuu ylitsepääsemättömiä ongelmia. (Ongelmia voi syntyä silloin kun konfiguraatio siirretään toiseen koneeseen, ja konfiguraatiossa on viittauksia ohjelmiin mitä ei toisessa koneessa ole).

Konfiguraatioon sisältyy mm.

- Laitteistoajureiden asetukset. Mitä laitteita työasemaan on kytketty, missä niiden ajurit ovat ja mitä parametrejä ajureille on määritelty.

- Windowsin asetukset. Minne Windows on asennettu, mikä on valittu näyttöresoluutio, jne.

- Asennettujen ohjelmien asetukset. Mitä ohjelmia on asennettuna, kaikkien ohjelmien konfiguraatiotiedot.
- Käyttäjäkohtaiset määrittelyt. Ikkunoiden paikat, valitut värit, taustakuvat jne.
- Program Managerin ikoni ja ohjelmaryhmä määritykset. Ikoneiden paikat. Program Managerin mahdolliset rajoitukset jne.

***Käyttäjäkohtaiset ympäristöt***

Käyttäjäkohtaisen ympäristön toteuttaminen vaatii luonnollisesti käyttäjien tunnistamista. Tavallisesti Windowsissa kaikki Windows-ympäristön määrittelevät asetukset ovat työasemakohtaisia.

Käyttäjien työpöydät ovat samannäköiset, ja jos yksi muuttaa jotain asetusta, vaikkapa työpöydän väriä tai taustakuvaa, niin se muuttuu kaikilla.

Jos halutaan että useampi käyttäjä pystyy käyttämään samaa konetta, tai että käyttäjän omat asetukset seuraavat käyttäjää, tarvitaan konfiguraationhallintaa. Eri käyttäjien asetukset on tallennettava jonnekin ja ne on vaihdettava samalla kun käyttäjä vaihtuu. Asetusten vaihtaminen ei ole ihan ongelmatonta, koska muutosten voimaan saattaminen voi vaatia Windowsin uudelleen käynnistämisen.

Ainoa käyttäjäkohtainen tieto mitä Windows normaalisti tallentaa on käyttäjien salasanalistat. Näitä salasanalistoja käytetään verkkoyhteyksien automaattiseen muodostamiseen. Salasanalistat sisältävät käyttäjien salasanoja eri verkkopalvelimiin, ja listat on suojattu käyttäjän omalla salasanalla, joka kysytään aina kun käyttäjä kirjottautuu sisään Windowsiin. Käytetty salausalgoritmi ei ole julkinen, ja sen on oltavan USA:n puolustusministerion vientirajoitusten mukainen. Tämä tarkoittaa sitä että käytetty salausavain saa olla korkeintaan 40 bittinen. Salasanalistaa ei voida pitää turvallisena jos sitä yritetään todella murtaa.

### 4.2.1. Käyttäjäkohtaisen konfiguraationhallinnan toteuttaminen

Konfiguraationhallinnan toteuttamiseen vaikuttaa paljon se, mitä halutaan saavuttaa. Voidaan haluta että eri käyttäjät voivat jakaa saman koneen niin, että kaikilla voi olla erilaiset konfiguraatiot. Tällöin konfiguraatiotiedot voidaan tallettaa kullekkin käyttäjälle paikallisesti kyseiseen työasemaan. Jos halutaan, että käyttäjät voivat pitää samat

konfiguraatiot eri tietokoneissa, pitää konfiguraatiotiedot tallettaa palvelimelle, mistä ne tarvittaessa haetaan kyseiseen tietokoneeseen.

### *Konfiguraatiotietoryhmät*

Konfiguraatiotietoa on monenlaista, eikä kaikki tieto ole käyttäjäkohtaista. Jos tietokoneilla on erilainen kokoonpano, työasemakohtaista tietoa ei ole hyvä siirtää koneesta toiseen. Eri koneet vaativat erilaisia laiteajureita, ja niiden siirtäminen koneesta toiseen aiheuttaa helposti ongelmia. Windowsin käynnistäminen väärillä laiteajureilla saa aikaan käynnistymisen epäonnistumisen, ja kone palaa DOS:n.

Käyttäjäkohtaisen ja tietokonekohtaisen konfiguraatiotiedon lisäksi voidaan erottaa myös muita tietokokonaisuuksia. Käyttäjät on yleensä jaettu *käyttäjäryhmiin* ja voidaankin haluta asettaa ryhmäkohtaista konfiguraatiotietoa. Samaa palvelinta käyttävät tietokoneet voivat myös jakaa yhteistä tietoa.

Käyttäjäkohtaista tietoa ovat esimerkiksi käyttäjän nimi, käyttäjän henkilökohtaiset ohjelmat ja niiden konfiguraatiotiedot jne. Konekohtaista tietoa ovat esim. käytetyt laiteajurit, tiedot koneen rakenteesta ja tietokoneen nimi. Tietokoneryhmäkohtaista tietoa olisi esimerkiksi palvelimeen kytketyn kirjoittimen tiedot. Käyttäjäryhmäkohtaista tietoa olisivat kaikki käyttäjäryhmän jäsenille yhteiset tiedot, esimerkiksi yhteiset ohjelmat jne. Lisäksi voidaan haluta määrittää kaikille yhteistä tietoa, mitä voitaisiin kutsua vaikkapa globaaliksi konfiguraatiotiedoksi.

Jotta konfiguraatiotiedot voitaisiin jakaa erilaisiin ryhmiin, sekä muodostaa konfiguraatiotiedostot tilanteen mukaan käyttäjästä ja koneesta riippuen, tarvitaan jokin järjestelmä tiedon lajittelemiseen. On pystyttävä sanomaan mihin ryhmään mikäkin tieto kuuluu, ja ryhmää on pystyttävä tarvittaessa muuttamaan. Olisi myös hyvä pystyä varmistamaan, että syntyneet konfiguraatiot ovat myös toimivia.

## *Konfiguraatioiden toimiminen*

Konfiguraatiotietojen hakeminen palvelimelta ei ole täysin ongelmatonta. Jos halutaan turvallisuutta Windows-työasemiin, on Windows pidettävä käynnissä koko ajan. DOS ei ole suojattu mitenkään. Koska Windowsin on oltava käynnissä, se on pitänyt käynnistää joillakin konfiguraatiotiedoilla Tässä vaiheessa ei kuitenkaan tiedetä seuraavaa käyttäjää, eikä näin ollen ole voitu hakea tämän käyttäjän tietoja. Toisaalta palvelimelle ei pääse hakemaan mitään tietoa ennen kuin sille on kerrottu kuka tietoa hakee ja annettu tarvittava salasana.

Windows voidaan käynnistää niillä konfiguraatiotiedoilla, jotka ovat olemassa edellisen käyttäjän jäljiltä. Tässä vaiheessa tietokoneen ruudulla on login-ikkuna, ja odotellaan että seuraava käyttäjä kertoisi käyttäjätunnuksensa ja salasanansa. Kun nämä tiedot on saatu, voidaan luoda verkkoyhteys palvelimelle ja käydä hakemssa kyseisen käyttäjän konfiguraatiotiedot. Nämä tiedot siirretään Windows työasemaan ja saatetaan asetukset voimaan kutsumalla Windows rutiineja, joilla asetuksia dynaamisesti muutetaan.

# 5. TeamWARE DeskTop

TeamWARE DeskTop (TWD) on ICL:n tuote, jolla pyritään ratkaisemaan Windowsin turvallisuus- ja konfiguraationhallinnan ongelmia. DeskTop on tavallaan Windows -käyttöjärjestelmän laajennus. (siinä määrin kun Windowsia voidaan pitää oikeana käyttöjärjestelmänä). Se kontrolloi Windows-työaseman käyttöä ja tarjoaa ylläpitäjälle hallitun ympäristön, jossa voidaan keskitetysti hallita työasemaverkkoon kuuluvia Windows-työasemia.

DeskTop:n tarkoituksena oli toteuttaa turvallinen ja hallittava Windows ympäristö.

*DeskTop on nimi ohjelmistolle, jolla toteutetaan turvallinen ja hallittu Windows-ympäristö.*

DeskTop mahdollistaa työasemien tehokkaan jakamisen eri käyttäjien kesken, siten että käyttäjän omat asetukset seuraavat käyttäjää. Ylläpidon ja konfiguraationhallinnan lisäksi DeskTop tarjoaa turvallisuusominaisuuksia Windows-työasemaan ja mahdollistaa ohjelmien automaattisen asennuksen ja kopioinnin työasemalle.

Turvallisuusominaisuuksissa tavoitteeksi asetettiin ITSEC:n C2 turvallisuusstandardi.

### *DeskTop ja verkkokäyttöjärjestelmä*

Suunnittelun yhtenä kriteerinä oli tuotteen toimivuus erilaisissa PC-verkkoissa. Työmäärän pienentämiseksi haluttiin että DeskTop ei tarvitsisi toimiakseen omaa prosessia palvelimelta. Eri verkkopalvelimien käyttöjärjestelmät ovat varsin erilaisia, ja ohjelmien tekeminen siten, että ne toimisivat kaikissa näissä verkkokäyttöjärjestelmissä ei ole täysin ongelmatonta. Sen sijaan kaikki verkkokäyttöjärjestelmät tarjoavat varsin samanlaisen liityntärajapinnan työasemalle. DeskTop toimii pelkästään työasemassa, ja hyödyntään verkkopalvelinta käyttäjien tunnistukseen ja tiedon tallentamiseen.

Windows ei tarjoa minkäänlaista käyttäjienhallintaa. Koska kaikki verkkokäyttöjärjestelmät tarjoavat käyttäjienhallinnan, niin oli luonnollista, että DeskTop hyödyntää verkkokäyttöjärjestelmää käyttäjienhallintaan identifiointiin ja autentikointiin. Hyvänä puolena on se, ettei ylläpitäjän tarvitse luoda uusia käyttäjiä useampiin paikkoihin.

Pääasialliset verkkokäyttöjärjestelmät, joita DeskTop tukee ovat Microsoft Networking (Mukaan lukien LAN Manager-ympäristöt, LAN Manager for OS/2, LAN Manager for

UNIX, Windows NT Server jne) ja Novell NetWare ympäristöt (NetWare 3.xx ja NetWare 4).

### *DeskTop ja Microsoft Networking*

Microsoft Networking:ssa DeskTop:lla luodaan palvelimeen oma jako (share). DeskTop:n käynnistyessä se yrittää etsiä palvelimesta TWD_CONF-nimistä jakoa. Jos tämä jako löytyy, DeskTop muodostaa sinne yhteyden ja käyttää siellä olevia konfiguraatiotietoja.

### *DeskTop ja NetWare 3*

NetWare 3:ssa palvelimet eivät ole toisistaan tietoisia. Kaikkiin palvelimiin joita halutaan käyttää pitää kirjoittautua sisään erikseen. DeskTop asennetaan johonkin palvelimista. Käyttäjän pitää kertoa sisäänkirjottautumisen yhteydessä mihin palvelimeen hän haluaa.

DeskTop:n kannalta ongelman muodostaa miten löytää DeskTop:n konfiguraatiotiedot palvelimesta. NetWare 3:ssa tämä tehdään siten että palvelimen pääkiintolevylle (sys-volume) tehdään TWD_CONF-niminen hakemisto jossa konfiguraatiotiedot ovat. Jos DeskTop halutaan asentaa jollekkin muulle kuin sys-volumelle, niin sys-volumen TWD_CONF hakemistoon tehdään tiedosto samalla nimellä, ja tähän tiedostoon kirjoitetaan miltä kiintolevyllä DeskTop:n tiedot löytyvät.

### *DeskTop ja NetWare 4*

DeskTop asennetaan yhteen puun haaraan, ja samalla sille nimetään palvelin, jonne kaikki konfiguraatiotiedot tallennetaan. Koska jokaisella haaralla ei välttämättä tarvitse olla nimettynä omaa palvelinta, luodaan aina siihen haaraan mihin DeskTop asennetaan alias-linkki. Linkki osoittaa DeskTop:n palvelimen sille partitiolle, johon DeskTop:n tiedot on tallennettu. Käyttäjän validioinnin ei tarvitse välttämättä tapahtua siitä puun osasta, johon DeskTop on asennettu, vaan käyttäjä voidaan tarvittaessa validioida myös muualta. Myös ylläpitäjä voi ylläpitää samasta kotiympäristöstään useita DeskTop ympäristöjä.

### *Site-käsite*

DeskTop toimii varsin erilaisissa verkkokäyttöjärjestelmissä, ja nämä verkko-käyttöjärjestelmät käyttävät varsin erilaista termistöä. Käsitteiden yhdenmukaistamiseksi DeskTop:ssa päätettiin käyttää käsitettä site.

*Site:llä tarkoitetaan käyttäjien ja käyttäjäryhmien joukkoa ja niiden konfiguraatiotietoja, joita hallitaan samasta paikasta.*

Site:n nimenä on se palvelin tai domain, jossa konfiguraatiotiedot sijaitsevat. LAN Manager ympäristössä sitenä toimii domain, NetWare 3:ssa palvelin ja NetWare 4:ssa se NDS puun osa, jossa käyttäjät on määritelty.

### *Työasemaryhmät*

*Työasemaryhmä on ylläpitäjien tekemä jako eri työasemien kesken. Aina kun DeskTop asennetaan johonkin työasemaan. Työasema liitetään johonkin työasemaryhmään.*

Työasemaryhmässä on yksi tai useampia työasemia. Työasemaryhmää käytetään automaattisen tiedostojen kopioinin totauttamiseen ja konfiguraatiotietojen luokitteluun. Ylläpitäjä laittaa samantyyliset työasemat samaan työasemaryhmään, esimerkiksi käyttötarkoituksen mukaan jaettuina.

# 5.1. Työpöytä

*Työpöytä on kaikki se mitä käyttäjä näkee kun Windows on käynnistynyt. Työpöytään kuuluvat kaikki ohjelma- ja ohjelmaryhmä- ikonit, kaikki erilaiset asetukset, joita käyttäjä on tehnyt tai joita ylläpitäjä on käyttäjälle määritellyt.*

Käyttäjät näkevät erilaiset konfiguraatiot työpöytien kautta. Työpöytä on nimi jollekkin konfiguraatiolle.

DeskTop:ssa käyttäjällä voi olla useita erilaisia työpöytiä, tai eri käyttäjillä voi olla erilaisia työpöytiä. Työpöydät on sidottu suoraan verkkopalvelimen käyttäjäryhmiin. Jokaisella ryhmällä, johon käyttäjä kuuluu, voi olla tallennettuna oma työpöytä.

Ylläpitäjät hallitsevat ja ylläpitävät työasemaverkkoa juuri työpöytien kautta. Ylläpitäjä pystyy valitsemaan ja käynnistämään haluamansa työpöydän konfigurointia varten. Työpöytää muutetaan samalla tavalla kuin yleensäkin Windowsin asetuksia ja ulkonäköä: asennetaan normaalisti ohjelmia, vaihdetaan värejä, asetetaan kirjoitinmäärittelyjä, muutetaan ohjelmien asetuksia, luodaan uusia ohjelmaryhmiä ja asetetaan ohjelmia käyttäjien saataville. Kun ylläpitäjä on saanut työpöydän näyttämään sellaiselta kuin hän haluaa, hän tallentaa työpöydän haluamalleen ryhmälle tai käyttäjälle.

*Työpöydän tallentaminen tarkoittaa että kaikki Windowsin konfiguraatiotiedostot (mm. ini- ja grp-tiedostot) tallennetaan verkkopalvelimelle.*

Myös DeskTopin omat asetukset, mukaanlukien turvallisuusasetukset, kuuluvat konfiguraatiotietoihin, eli nekin tallennetaan työpöytien mukana.

### *DeskTop ja loppukäyttäjät*

Loppukäyttäjille DeskTop on lähes läpinäkyvä. Käyttäjät käyttävät Windows työasemaansa aivan samalla tavalla kuin jos työasemassa ei olisi DeskTop:a asennettuna. Näkyvin ero käyttäjälle on se, että hänen on mahdotonta päästä käyttämään työasemaansa ilman että hänet on autentikoitu. Tietysti käyttäjä huomaa DeskTop:n olemassaolon jos hän yrittää tehdä jotain mikä on häneltä kiellettyä.

Aina kun käyttäjä haluaa käyttää Windows-työasemaansa vaaditaan, että hänen on kirjottauduttava sisään työasemaansa (autentikointi). Näin varmistetaan että käyttäjä on aina tunnettu. Kirjottautuminen tehdään itseasiassa verkkopalvelimelle. Jos kirjottautuminen verkkopalvelimelle ei onnistu, ei käyttäjä pääse myöskään käyttämään

konettaan. Tätä vaatimusta ylläpitäjät voivat tosin lieventää sallimalla paikallisen validioinnin. Tällöin verkkoyhteyden puuttuessa käyttäjä validioidaan perustuen työasemaan tallennettuihin tietoihin.

Normaalisti Windows-työasemassa työpöytä on konekohtainen, ja jos käyttäjä menee eri tietokoneelle hän saa käytettäväkseen sen konfiguraation, joka sattuu olemaan siinä tietokoneessa. DeskTop:ssa sensijaan käyttäjän oma konfiguraatio eli työpöytä seuraa häntä kaikkiin koneisiin. Jos käyttäjä menee eri tietokoneelle kuin tavallisesti, hänen työpöytänsä haetaan verkon palvelimelta ja asetetaan käyttöön.

Jos käyttäjälle on määritelty useita työpöytiä, voi hän valita haluamansa, muussa tapauksessa automaattisesti käynnistetään määritelty työpöytä. Jos käyttäjälle ei ole määritelty mitään työpöytää, käynnistetään asennuksen yhteydessä luotu *Default-työpöytä*. Default-työpöytää käytetään niille käyttäjille, joille ei löydy mitään muuta työpöytää.

Tätä ominaisuutta voidaan käyttää hyväksi myös silloin kun järjestelmässä ei tarvita useita työpöytiä.

Halutessaan ylläpitäjä voi myös sallia käyttäjän tekemien omien muutosten tallentamisen. Toistaalta ylläpitäjä voi myös pakottaa käyttäjän käyttämään tiettyä työpöytää, jos se katsotaan tarpeelliseksi. Esimerkiksi jos työasema toimii pankkikonttorin kassakoneena, voi olla tarkoituksenmukaista, että kaikilla työntekijöillä on identtinen työpöytä määriteltynä siten, että käyttäjät eivät pysty muuttamaan mitään. Sellaisissa tapauksissa tietokoneella ajetaan yleensä vain yhtä sovellusta.

## 5.2. DeskTop ja turvallisuus

DeskTop:n turvallisuustavoitteena on ITSEC:n F-C2 turvallisuuskriteeri. Turvallisuuskriteerin vaatimukset on esitelty aikaisemmin.

DeskTop:n turvallisuus perustuu oikeuksien kieltämiseen. Kaikki turvallisuusasetusten kiertämisen mahdollistavat toiminnot on estettävä. Yleisessä tapauksessa se ei ole mahdollista, mutta useissa erityistapauksissa se onnistuu, aiheuttamatta käyttäjille kohtuutonta haittaa. DeskTop:a voi luonnehtia siis toiminnoiltaan rajoitetuksi ympäristöksi.

DeskTop:n käyttäminen on mielekästä vain sellaisissa ympäristöissä, joissa on mahdollista määritellä tarkasti käyttäjien tarvitsemat sovellusohjelmat ja joissa ylläpitäjät voivat koota käyttäjille heidän tarvitsemansa kokonaisuudet. Tälläinen lähestymistapa toimii hyvin silloin kun tietokoneita käytetään vain jonkun tietyn ohjelman suorittamiseen (esim. päätteenä pankin keskustietokoneeseen) tai kun käyttäjien ohjelmat pystytään helposti luettelemaan. Tavallisessa toimistoympäristössä ohjelmistojen luetteleminen on mahdollista.

DeskTop:n turvallisuus vaatii seuraavia olettamuksia:

- *Palvelin on turvallinen.*
- *Työasema ei tunnista palvelinta. Turvallisuusaukko syntyy jos joku kytkee työaseman toiseen palvelimeen, jossa on saman nimisiä käyttäjätunnuksia.*
- *Työasema on suojattu fyysisesti niin, että sen kiintolevyyn ja BIOS:kseen ei pääse käsiksi.*
- *Järjestelmä on asennettu niin että käyttäjät eivät saa asennetua käyttöönsä uusia ohjelmia.*

Seuraavassa käydään läpi DeskTop:n turvallisuusominaisuudet.

### *Toimenpiteet ennen Windowsin käynnistystä*

Jotta Windows-työasemassa voitaisiin puhua minkäänlaisesta turvallisuudesta, on käyttäjää estettävä pääsemästä DOS:n. Mikäli käyttäjä pääsee käyttämään tietokonetta DOS:sta, pystyy hän ohittamaan kaikki turvallisuusominaisuudet.

DOS suorittaa käynnistyessään autoexec.bat nimistä komentotiedostoa. Tämän komentotiedoston suorittaminen on kuitenkin mahdollista keskeyttää lähettämällä koneelle control-c merkkejä.

*Kun DeskTop asennetaan työasemaan, asennetaan samalla Windows käynnistymään automaattisesti. Control-c merkkien lähettäminen estetään ajamalla heti ensimmäiseksi ohjelma, joka ottaa vastaan kaikki näppäimistön painallukset eikä laske niitä DOS:lle.*

Jos Windowsin käynnistyminen jostain syystä estyy, ei koneella pysty tekemään mitään, koska näppäimistöltä ei pysty kirjottamaan.

Ongelmaksi jää se, että tietokone voidaan käynnistää DOS-käynnistyslevykkeeltä. Tätä ongelmaa ei pystytä korjaamaan ohjelmallisesti, vaan se vaatii että tietokoneen BIOS:sta voidaan asettaa kone käynnistymään aina kovalevyltä ja että BIOS voidaan suojata salasanalla.

### 5.2.1. Autentikointi ja Identifiointi

Kaikki DeskTop:n kanssa toimivat verkkokäyttöjärjestelmät tarjoavat hyvät käyttäjienhallinta ominaisuudet. Samalla ne tarjoavat myös hyvän mekanismin käyttäjien autentikointiin. Verkkokäyttöjärjestelmät vaativat jokaiselta käyttäjältä oman ja yksiselitteisen tunnuksen. DeskTop:ssa käyttäjienhallinta ja autentikointi ovat verkkokäyttäjärjestelmän vastuulla.

Työasemakohtaisesti voidaan asettaa sallittu pienin oikeustaso, jolla sisäänkirjottautuminen hyväksytään. Mahdollisia vaihtoehtoja ovat: työaseman omistaja, ylläpitäjä, autentikoitu käyttäjä tai vieras.

- Työaseman omistaja on se henkilö, jolle kyseinen työasema on merkitty. Jos tämä on ainoa sallittu sisäänkirjottautumisen taso, on hän ylläpitäjien lisäksi ainoa käyttäjä, joka pystyy käyttämään kyseistä työasemaa.

- Autentikoiduilla käyttäjillä tarkoitetaan niitä käyttäjiä, jotka verkkopalvelin pystyy tunnistamaan. Näiden käyttäjien on pystyttävä antamaan oikea käyttäjätunnus ja salasana ennenkuin tietokoneen käyttö on sallittua.

- Verkkokäyttöjärjestelmät voivat antaa myös vierailleen käyttöoikeuden. Vieras on käyttäjätunnus, jota palvelin ei tunne, tai ennalta määrätty tunnus, jolla ei yleensä ole salasanaa. Jos vierailla on oikeus käyttää konetta, myös käyttäjät joita ei ole

määritelty palvelimessa saavat käyttää konetta. Kaikki muut turvallisuusasetukset ovat voimassa tavalliseen tapaan.

Sisäänkirjottautumisprosessi on kuvattuna yhdessä konfiguraation lataamisen kanssa kuvissa 7 - 10.

Ennenkuin käyttäjä pystyy suorittamaan mitään ohjelmia on hänen annettava käyttäjätunnus ja hyväksytysti kirjoittauduttava sisään palvelimelle. Jos käyttäjällä on resursseja käytössä useammista palvelimista, DeskTop hoitaa sisäänkirjottautumisen niihin kaikkiin. Tätä ominaisuutta kutsutaan single login:ksi. Käyttäjä kirjottautuu sisään vain kerran, minkä jälkeen järjestelmä huolehtii sisäänkirjottautumisesta muihin järjestelmiin. Tämä on toteutettu siten, että DeskTop pyrkii synkronoimaan kaikki salasanat samoiksi. Jos sisäänkirjottautuminen johonkin resurssiin epäonnistuu, kysytään salasana käyttäjältä.

Sisäänkirjottautumisen yhteydessä käyttäjä voi valita sen site:n, jota hän haluaa käyttää. Ylläpitäjät voivat määrittää työasemakohtaisesti sallitut sisäänkirjottautumis site:t. NetWare 4 ympäristössä site-nimet voivat olla hyvinkin pitkiä, ja tätä helpottamaan ylläpitäjät voivat määritellä alias-nimiä site:ille.

## *Salasanat*

Sisäänkirjottautumisen validioinin DeskTop jättää verkkokäyttöjärjestelmän tehtäväksi; samalla verkkokäyttöjärjestelmä huolehtii salasanojen minimivaihtoväleistä ja -pituuksista. DeskTop on kuitenkin tietoinen salasanojen vaihtamisesta, ja mikäli salasana vaihdetaan yhdessä järjestelmässä, yrittää DeskTop automaattisesti vaihtaa sitä myös muissa. Ylläpitäjä voi myös määrittää DeskTop:n karsimaan liian helppoja salasanoja.

Liian helppojen salasanojen tunnistamista varten DeskTop:iin voidaan määrittää listoja kielletyistä salasanoista ja niiden osista. Kun käyttäjä vaihtaa salasanaansa, DeskTop varmistaa, että salasana on hyväksyttävä, ennen kuin se suostuu vaihtamaan salasanan itse palvelimeen.

DeskTop koukuttaa ("hooking", käsitelty aikaisemmin) ne funktiot, joilla verkkokäyttöjärjestelmän salasanat voidaan vaihtaa. Se tehdään siksi, että DeskTop voi tarkistaa helppoja salasanoja, ja tarvittaessa vaihtaa salasanoja myös muihin järjestelmiin, joihin käyttäjä on yhteydessä.

### *Paikallinen autentikointi*

Jos palvelin ei ole toiminnassa tai ei jostain syystä vastaa, voi järjestelmän ylläpitäjä haluttaessaan sallia autentikoinin myös paikallisesta työasemasta. Käyttäjien salasanat ovat tallennettuina yhteensuuntaan salattuina työasemassa. Yhteensuuntaan salaaminen on toteutettu salaamalla salasana FEAL-salausalgoritmilla /11/ käyttäen avaimena salasanaa itseään. Näin salatut salasanat tallennetaan työasemaan DeskTop:n hakemistoon. Tähän tiedostoon käyttäjillä ei ole mitään oikeuksia.

DeskTop tallentaa konfiguraatiotiedot paikalliselle kovalevylle, joten jos verkkoyhteyttä ei pystytä luomaan, voidaan tiedot ladata paikallisesti. Konfiguraatiotietojen paikallinen tallentaminen ei paranna ainoastaan toimintavarmuutta verkon ongelmatilanteissa, vaan myös suorituskykyä, koska tietojen hakeminen paikalliselta kovalevyltä on huomattavasti nopeampaa kuin palvelimesta.

### *Toimikortit*

DeskTop tulee myös tukemaan toimikorttien käyttämistä autentikointiin. Toimikortti on pieni tietokone joka on istutettu luottokortin kokoiselle muovin kappaleelle. Toimikorttille voidaan tallettaa turvallisesti tietoa. Toimikortille tallennettua tietoa on lähes mahdotonta saada selville ulkopuolelta.

Toimikortin rakenne on seuraava. Kommunikoivien osapuolten pitää tunnistaa toisensa voidakseen hakea tai tallettaa tietoa toimikortin muistista. Sen jälkeen toimikortille voidaan esittää komentoja, ja kortti tutkii onko komento sallittu ja tarvittaessa toteuttaa sen. Toimikortti on hyvä ja turvallinen paikka esimerkiksi salasanojen tallentamiseen.

DeskTop:ssa toimikorttia tullaan käyttämään käyttäjätunnusten ja salasanojen tallentamiseen. Pystyäkseen käyttämään työasemaansa on käyttäjän annettava toimikorttinsa kortinlukijaan. DeskTop pyytää salasanan käyttäjältä, avaa salasanalla toimikortin, hakee käyttäjätunnuksen kortilta, ja autentikoi käyttäjän palvelimelle. Ylläpitäjä voi halutessaan sallia työaseman käytön vain toimikortilla. Tällöin ei riitä, että käyttäjä tietää salasanansa, vaan hänellä on myös oltava kortti mukana. Itse salasanan selville saaminen ei riitä työasemaan murtautumiseen. Sen sijaan salasana on riittävä palvelimen resurssien käyttöoikeuden saamiseen.

## 5.2.2. Automaattinen sisäänkirjottautuminen muihin järjestelmiin

### *Eri verkkojen käyttäminen samanaikaisesti*

Windows-työasema voidaan asentaa käyttämään useampia verkkoja ja verkkoprotokollia samanaikaisesti. Eri verkkoja voi olla kaksi: primary- ja secondary verkko. Erilaisia verkkoprotokollia voi puolestaan olla useita (Netbios, IPX, TCP/IP jne). Yleensä Microsoftin verkko toimii primary-verkkona.

DeskTop voi käyttää toisena verkkona NetWare:a. Tällöin käyttäjä pystyy hakemaan palveluita sekä NetWare, että LAN Manager palvelimista samaan aikaan. Koska eri arkkitehtuureihin kuuluvat palvelimet eivät ole tietoisia toisistaan, niihin joudutaan kirjottautumaan sisään erikseen. Käyttäjälle se tietysti aiheuttaa ylimääräistä vaivaa, ja tästä syystä DeskTop automatisoi eri palvelimiin tapahtuvan sisäänkirjottautumisen.

Työaseman käynnistyessä käyttäjältä kysytään käyttäjätunnus ja salasana, joita käytetään kirjottauduttaessa sisään palvelimelle. Jos käyttäjä on määritellyt tai hänelle on määritelty yhteyksiä muihin palvelimiin, DeskTop yrittää automaattisesti kirjottautua sisään käyttäen samaa käyttäjätunnusta ja salasanaa. Jos sisäänkirjottautuminen epäonnistuu, DeskTop pyytää käyttäjää antamaan käyttäjätunnuksen ja salasanan. Jos käyttäjän antama käyttäjätunnus on sama kuin pääasialliseen palvelimeen sisäänkirjottautumisen yhteydessä käytetty tunnus, DeskTop synkronoi salasanat samoiksi. Jos taas käytetty käyttäjätunnus ei ole sama, DeskTop tallettaa sekä käyttäjätunnuksen että salasanan tiedostoon salattuna FEAL algoritmilla. Salaukseen tarvittava avain generoidaan käyttäjän alkuperäisestä salasanasta.

Jos sisäänkirjottautuminen epäonnistuu, DeskTop kysyy automaattisesti salasanaa käyttäjältä. Uusi salasana tallennetaan automaattisesti.

### *Pääte-emulaattorituki*

Yrityksillä on usein käytössään isoja IBM-mainframe-, tai erilaisia UNIX-tietokoneita. Näitä isompia tietokoneita käytetään pyörittämään isoja tietokantoja, tai niissä saattaa sijaita esimerkiksi jonkin vanha tietojärjestelmä.

Käyttäjät ajavat Windows-koneessaan pääte-emulaattoria, jolla he saavat yhteyden kohdekoneisiin. UNIX ja IBM-mainframe-tietokoneet vaativat käyttäjän autentikoinnin ennen kuin päästävät käyttäjän käsittelemään tietojaan. Käyttäjällä on olemassa

käyttäjätunnus ja salasana myös näihin koneisiin. Salasanalla voi olla erilaiset vaatimukset, ja ne voivat esimerkiksi vanhentua automaattisesti.

DeskTop hoitaa automaattisen sisäänkirjottautumisen eri palvelimiin, ja ylläpitäjät haluavat tarjota samaa helppokäyttöisyyttä myös pääte-emulaattoreiden kanssa. Myös pääte-emulaattoreiden valmistajat ovat tietoisia tästä toiveesta, ja useimmat pääte-emulaattoriohjelmat sisältävät ohjelmointitukea ja erilaisia komentojonotiedostoja (scriptejä). Scriptien lisäksi voidaan kirjoittaa erityisiä ohjelmia, joilla sisäänkirjottautuminen toteutetaan. Tavallisesti näitä ohjelmia kirjoitetaan esimerkiksi Visual Basic:lla.

DeskTop tarjoaa API-funktioita käyttäjätunnusten ja salasanojen turvalliseen säilyttämiseen. Käyttäjätunnus- ja salasanalistoja on myös mahdollista siirtää koneesta toiseen, ja DeskTop:a käytettäessä sama toiminnallisuus säilyy vaikka käyttäjä käyttäisi eri tietokoneita.

### *HLL-tuki*

IBM-mainframe tietokoneisiin pidetään yhteyttä 3270-päätteiden kautta. Usein 3270-päätteet on korvattu 3270-emulaattoreilla, joita ajetaan erilaisissa ympäristöissä. IBM kehitti 3280-emulaattoreita varten HLL-kielen (High Level Language), joka mahdollistaa pääte-emulaattorin kanssa keskustelemisen. Yleisimmistä 3270-emulaattoreista löytyy tuki HLL-kielelle.

HLL:n avulla on mahdollista lukea tilannetietoa pääte-emulaattorilta, selvittää mitä ruudulla lukee ja lähettää tietoa keskuskoneelle.

DeskTop tarjoaa myös API-funktiokutsuja, jotka mahdollistavat keskustelun erilaisten 3270-pääte-emulaattoreiden kanssa HLL:ä käyttämällä. DeskTop:in funktioiden avulla voidaan etsiä ruudulta merkkijonoja, jotka ovat määriteltävissä säännöllisillä lausekkeilla (regular expression).

### *DDE-tuki*

Dynamic data exchange (DDE) on Windowsin tarjoama ratkaisu prosessien väliseen kommunikointiin. DDE:n avulla prosessit pystyvät keskustelemaan keskenään käyttäen hyväkseen jaettua muistia. DDE:tä voi käyttää paitsi kerran tapahtuviin tiedon siirtoihin, myös jatkuvaan tiedonsiirtoon, jossa tietoa välitetään heti kun sitä tulee saataville.

### *DDE:n rakenne*

Tiedonsiirto tapahtuu aina asiakas- ja palvelinsovelluksen välillä. Asiakassovellus aloittaa tiedonsiirron avaamalla keskustelun palvelinsovelluksen kanssa. Keskustelussa asiakassovellus voi pyytää tietoa tai palveluita palvelinsovellukselta. Saatuaan pyynnön jostain toimenpiteestä, palvelinsovellus vastaa siihen ja palauttaa asiakassovellukselle tämän pyytämän tiedon tai mahdollisesti suorittaa pyydetyn palvelun. Palvelinsovellus voi samanaikaisesti palvella useita asiakkaita. Sovellus voi myös toimia samanaikaisesti sekä palvelimena että asiakkaana. Asiakkaan velvollisuutena on keskustelun päättäminen, kun sitä ei enää tarvita.

DDE-palvelin käyttää kolmitasoista hierarkiaa määrittelemään tarkasti mistä tiedosta tai palvelusta halutaan keskustella. Ylimpänä tasona on palvelunnimi (Service name). Palvelunimi on merkkijono, johon palvelinsovellus vastaa kun asiakassovellus yrittää aloittaa keskustelua. Palvelin voi vastata myös useisiin erilaisiin palvelunnimiin - vaikka yleensä palvelimet vastaavat vain yhteen nimeen.

Palvelunimen jälkeen määritellään aihe (Topic). Aihe kertoo sen loogisen aihepiirin, johon keskustelu kohdistuu. Tiedostopohjaisissa dokumenteissa toimimilla palvelimilla aiheena on useinmiten tiedostonimi, muun tyyppisillä sovelluksilla aiheina ovat erilaiset sovelluskohtaiset merkkijonot. Asiakassovellus kertoo aiheen aina keskustelua aloitettaessa.

Alimpana tasona on kohde (Item ). Kohde määrittelee tiedon, jonka palvelin voi palauttaa asiakkaalle keskustelun aikana. Esimerkiksi kohde voi olla kokonaisluku, kuva tai useita kappaleita tekstiä.

DDE määrittää myös erityisen aiheen nimeltään system-aihe. Tätä aihetta asiakassovellukset voivat käyttää selvittämään mitä palveluita on tarjolla ja minkälaista tietoa nämä voivat tarjota.

### *DDE ja DeskTop*

DeskTop hyödyntää DDE:tä erilaisten käyttäjätunnus- ja salasanatietojen käsittelemiseen. Monet pääte-emulaattorit tukevat DDE:ä ja DeskTop:n DDE tuki mahdollistaa salasanojen turvallisen säilyttämisen ja siirtämisen eri tietokoneisiin. DeskTop toimii sekä DDE-asiakkaana että DDE-palvelimena.

### *DeskTop DDE-palvelimena*

DeskTop:n toimiessa DDE-palvelimena muut sovellukset (asiakkaat) voivat käyttää sitä käyttäjätunnusten ja salasanojen tallentamiseen. Tarvittaessa ne ottavat DeskTop:iin yhteyttä ja pyytävät sitä antamaan tiettyyn yhteyteen liittyvät tiedot..

Lisäksi asiakkaana toimiva sovellus voi pyytää DeskTop:a kysymään käyttäjältä käyttäjätunnuksen ja salasanan. Asiakas voi myös pyytää DeskTop:a tallettamaan käyttäjätunnuksia ja salasanoja. DeskTop automaattisesti salaa tiedot FEAL-algoritmilla.

Toiminan ajatuksena on, että pääteohjelma suorittaa jotain komentojonotiedostoa, jolla tehdään automaattinen sisäänkirjoitus esimerkiksi UNIX-koneeseen. Pääteohjelma odottaa ruudulta tarvittavia tietoja, esimerkiksi milloin Unix-kone pyytää käyttäjätunnusta ja salasanaa. Tällöin pääteohjelma ottaa DDE:n kautta yhteyden DeskTop:n ja kysyy ko. järjestelmän tietoja. Jos näitä tietoja ei ole, voi pääteohjelma kysyä itse käyttäjältä käyttäjätunnuksen ja salasanan tai pyytää DDE:n kautta DeskTop:ia kysymään käyttäjältä ko. tiedot. Jos sisäänkirjottautuminen epäonnistuu, kysytään tietoja käyttäjältä uudestaan. Tarvittavat komentojonotiedostot ovat sekä emulaattori-, että kohdekone kohtaisia. Toisaalta ne eivät ole kovin pitkiä, ja niitä on varsin helppo tehdä.

### *DeskTop DDE-asiakkaana*

Automaattinen sisäänkirjottautuminen voidaan myös suorittaa siten, että DeskTop toimii DDE-asiakkaana. Tällöin rakennetaan esimerkiksi Visual Basic ohjelma, jonka kautta DeskTop:n DDE-funktioita kutsutaan. Nämä funktiot puolestaan komentavat pääte-emulaattoria DDE:tä käyttäen.

DeskTop:n DDE-funktioiden kautta on mahdollista keskustella pääte-emulaattorin kanssa: etsiä sen ruudulta haluttuja merkkijonoja ja tarvittaessa antaa käyttäjätunnuksia ja salasanoja.

Esimerkiksi pääteohjelmaa käytettäessä voidaan tehdä Visual Basic ohjelma, joka odottaa tiettyä merkkijonoa DeskTop:n kautta. DeskTop mahdollistaa merkkijonojen määrittelyn säännöllisinä lausekkeina, joten on mahdollista tehdä hyvinkin monimutkaisia odotuskomentoja. Kun haluttu merkkijono löydetään, syötetään kysytty käyttäjätunnus ja salasana.

***DeskTop ja API:t***

DDE- ja HLL-tuen lisäksi DeskTop:n tarjoamia käyttäjätunnuksen ja salasanan käsittelyfunktioita voidaan kutsua myös tavallisista ohjelmista. Tarvittaessa ylläpitäjät voivat siis rakentaa oman ohjelman, joka hyödyntää DeskTop:in salasanojen automaattista siirtämistä käyttäjän mukana koneesta toiselle.

Tarkoituksena on tarjota rajapinnat, joita käyttämällä ylläpitäjät voivat automatisoida käyttäjien sisäänkirjottautumista muihin järjestelmiin.

## 5.2.3. Näytönsäästäjä

Windowsin näytönsäästäjän tehtävä on suojella näyttöä pimentämällä se silloin, kun työasemaa ei käytetä. Näytönsäästäjä käynnistyy automaattisesti ennalta säädetyn ajan kuluttua. Normaalisti käyttäjä saa itse valita käynnistymisajan, mutta DeskTopin avulla ylläpitäjä pystyy pakottamaan hyväksyttävän maksimiajan, jota suurempaa aikaa käyttäjä ei voi valita. Näytönsäästäjän käynnistettyä ruutu pimennetään, eikä ruudulta pysty lukemaan mitä siinä on. Näytönsäästäjän sammuttamiseksi käyttäjän on annettava salasana uudelleen.

Näytönsäästäjästä on aina mahdollista päästä eroon sammuttamalla kone ja antamalla sen käynnistyä uudelleen. Silloin tietysti kaikki tallentamaton tieto katoaa. Koska sähkön katkaisemisen estäminen on ohjelmallisesti varsin vaikeaa, voidaan haluttaessa sallia, logoutin suorittaminen näytön pimentimen päällä ollessa, minkä jälkeen palataan takaisin login ikkunaan. Logoutia suoritettaessa yritetään ensiksi sulkea kaikki avoimena olevat ohjelmat. Ohjelmien kysyessä varmistuskyselyjä käyttäjältä, ne näytetään, ja uusi käyttäjä pystyy niihin vastaamaan. Lisäksi ylläpitäjä voi päättää, että ylläpitäjät tai samaan ryhmään kuuluvat käyttäjät voivat poistaa näytön säästäjän. Myös tässä tapauksessa uusi käyttäjä autentikoidaan ja sisäänkirjoitetaan järjestelmään samalla kun edellinen käyttäjä pakotetaan ulos järjestelmästä.

Sekä varsinaisissa sisäänkirjottautumisissa että näytön säästäjä-lukon poistamisyrityksissä DeskTop pitää kirjaa siitä, montako epäonnistunutta yritystä on tehtynä. Näiden yritysten lukumäärä näytetään seuraavan onnistuneen sisäänkirjoittautumisen yhteydessä. Ylläpitäjällä on mahdollisuus määrittää tietokone lukittumaan, jos epäonnistuneita yrityksiä on liian paljon. Lukittua tietokonetta ei pääse käyttämään; siihen ei sallita edes sisäänkirjottautumisia. Lukitus poistuu automaattisesti seuraavana päivänä.

## 5.2.4. Tiedosto-oikeudet

DOS:n käyttämä FAT-tiedostojärjestelmä ei tarjoa mitään mahdollisuutta tiedosto-oikeuksien totauttamiseen, joten tiedosto-oikeudet on toteutettava jotenkin muuten.

DOS:ssa ja Windowsissa on mahdollista saada kiinni kaikki funktiokutsut, jotka kohdistuvat tiedostoihin. DeskTop käynnistää TWDACM.386-ajurin Windowsin käynnistämisen yhteydessä, jonka tehtävnä on huolehtia tiedosto-oikeuksista. Aina kun yritetään tehdä jotain tiedostolle, ajuri tarkistaa olemassa olevat oikeudet ja päättää sallitaanko operaatio vai ei.

Koska kaikki tiedosto-operaatiot kulkevat tämän käsittelijän kautta, siitä aiheutuu tietysti jonkin verran ylimääräistä kuormaa, ja tiedostojen käsittelynopeudet putoavat. Hidastuminen ei tosin ole havaittavissa, paitsi jos määriteltyjä tiedosto-oikeuksia on hyvin paljon.

Usein tiedostojen oikeudet on tallennettu tiedostojärjestelmään tiedostojen yhteyteen. Mutta koska FAT ei tarjoa tälläisiä ominaisuuksia joudutaan sama toiminnallisuus järjestämään muuten. Tiedosto-oikeuksien toteuttamiseen on useita vaihtoehtoja. Yksi mahdollisuus olisi rakentaa kokonaan oma tiedostojärjestelmä, joka tukisi tiedosto-oikeuksia. Tämän vaihtoehdon toteuttaminen on teknisesti hyvin vaikeaa DOS:ssa, ja huonona puolena on, että tiedostojärjestelmiä käsittelevät työkalut ( kuten doublespace; automaattinen tiedostojen pakkaus, erilaiset levyjen korjausohjelmat; chkdsk, Norton Diskutilities, defrag jne.) eivät toimisi. Toinen, helpompi vaihtoehto olisi tallettaa tiedosto-oikeudet itse tiedostoon, esimerkiksi tiedoston alkuun. Silloin tiedostojen käsittely hidastuu varsin paljon, ja tiedostojen käsitteleminen ilman asianomaista ajuria ei onnistu. Esimerkiksi mitään ohjelmatiedostoja ei voitaisi suorittaa, jos tiedostoajuri ei olisi toiminnassa. Kolmas vaihtoehto on että tiedosto-oikeudet tallennetaan johonkin muuhun paikkaan, ja aina kun tiedostoihin viitataan oikeudet tarkistetaan.

*DeskTop:ssa tiedosto-oikeudet tallennetaan tavalliseen ini-tiedostoon. Tiedosto-oikeus määritellään tiedostolle tai hakemistolle polkuineen, ja niille määritellään oikeus-ryhmät ja ryhmälle asetetut oikeudet. Myös tämä tiedosto on suojattu käyttäjiltä tiedosto-oikeuksien avulla. Käyttäjät eivät pysty muuttamaan tätä tiedostoa.*

### *Tiedosto-oikeus ryhmät*

DeskTop:ssa tiedosto-oikeuksia voidaan määritellä monille erilaisille ryhmille. Erikseen on määritelty kolme erityisryhmää:

1. Workstation Owner - työaseman omistaja, henkilö joka on merkitty työaseman haltijaksi.

2. Everyone - kaikki käyttäjät, mukaan lukien mahdolliset vierailijat (vieras on käyttäjä, jota ei ole autentikoitu palvelimelle).

3. Users - autentikoidut käyttäjät. Erityisryhmien lisäksi oikeuksia voidaan määritellä kaikille ryhmille ja käyttäjille erikseen. Ryhmät ja käyttäjät ovat samat kuin tiedostopalvelimen ryhmät ja käyttäjät.

Tiedosto-oikeudet on DeskTop:ssa sidottu polkuun ja tästä syystä ne toimivat hieman omalaatuisesti. Jos tiedosto kopioidaan paikasta toiseen, sen oikeudet eivät kopioidu tiedoston mukana. Tämä on varsinkin käyttäjille varsin hämäävää, ja he unohtavatkin sen helposti. Esimerkiksi on voitu määritellä tiedosto oikeus c:\windows\mytest.txt:ille, jos mytest.txt kopioidaan toiseen paikkaan hakemistopuussa, tiedosto-oikeus ei kopioidu mukana. Toisaalta voidaan määrittää oikeuksia myös tiedostoille ja hakemistoille, joita ei ole vielä olemassa. Oikeudet kohdistuvat välittömästi kyseiseen tiedostoon kun se syntyy.

DeskTop sallii oikeuksien määrittelyjen sisältävän villikortteja. Nämä oikeudet saadaan myös periytymään eripuolelle tiedosto puuta automaattisesti. Voidaan siis määritellä yhdellä komennolla kaikkien tietyn muotoisten tiedostojen oikeudet. Tämä on hyvin käyttökelpoinen ominaisuus ja vähentää huomattavasti tarvetta asettaa oikeuksia kaikille tiedostoille. Yleensä riittää kun asetetaan oikeuksia vain eri tiedostotyypeille. Nämä määrittelyt eivät ole riippuvaisia polusta, ja näin ollen oikeudet pysyvät vaikka tiedosto kopioitaisiin muualle. Taulukossa 1 on lueteltu DeskTop:ssa käytetyt tiedosto-oikeuksien tyypit.

Tiedosto-oikeus voi olla määriteltynä esimerkiksi *.doc = R, jolloin käyttäjä saa lukea kaikkialla olevia doc:iin päättyviä tiedostoja, mutta ei pysty muuttamaan niitä. Tietysti käyttäjällä usein on myös omia dokumentteja. Siksi onkin mielekkäämpää, että esimerkiksi käyttäjillä on vain lukuoikeudet yhteisiin dokumentteihin, mutta omia dokumenttejaan he saavat muokata vapaasti.

| | | |
|---|---|---|
| Read | Lukuoikeus | Käyttäjällä on oikeus pelkästään lukea tiedostoa. Tiedoston kopiointi on sallittua. |
| Write | Kirjoitusoikeus | Käyttäjä voi luoda uusia tiedostoja ja lisätä vanhoihin tietoa. |
| Execute | Suoritusoikeus | Käyttäjä voi ajaa tiedoston ohjelmana. Execute only tiedostoa ei voi kopioida muualle. |
| Delete | Tuhoamisoikeus | Käyttäjä voi poistaa tiedoston. |

Taulukko 1

DOS:ssa ja Windowsissa kaikki verkkoasemat näkyvät samanlaisina kuin varsinaiset kovalevytkin. Näin ollen DeskTop:ssa asetetut tiedosto-oikeudet toimivat myös verkon asemilla. Kaikkissa verkkokäyttöjärjestelmissä on jo itsessään tiedosto-oikeusmäärittelyt, joten DeskTop tarjoaa lähinnä yhdenmukaisen käyttäytymisen ja näkymän palvelimen resursseihin. DeskTopin määrittelyt eivät luonnollisestikaan pysty ohittamaan palvelimen omia määrittelyjä.

Pelkkä suoritusoikeus on varsin harvinainen ominaisuus Windows-ympäristöissä. Verkkokäyttöjärjestelmä ei tiedä mitä tarkoitusta varten Windows-työasema ohjelmatiedostoa lukee. Jos käyttäjillä on oikeus kirjoittaa tiedostoja verkopalvelimen levylle, ei verkkopalvelimelta pystytä estämään näiden ohjelmien ajamista. DeskTop:in toteutus puolestaan rakentaa ylimääräisen kerroksen Windows-työaseman puolelle, ja tiedosto-oikeuksia tarkastettaessa ei tehdä mitään eroa sille missä ohjelma fyysisesti sijaitsee. Ylläpitäjät voivat siis antaa käyttäjille lukuoikeuksia verkkolevyille, ilman että käyttäjät voivat suorittaa sieltä ohjelmia.

### *Oletusoikeudet*

Asennuksen yhteydessä DeskTop asettaa valmiiksi useita oikeuksia. Näistä tärkeimpänä ovat jokaisen tiedoston jonkinlaiset "perusoikeudet". Ne annetaan määrittelemällä *.*-

villikortti ilmaisulle kaikille autentikoiduille käyttäjille luku-, kirjoitus- ja tuhoamisoikeudet (RWD), sekä kaikille käyttäjille lukuoikeudet (R). Jos toisin ei ole sanottu saadaan siis yleensä lukea ja kirjottaa kaikkia tiedostoja. Näitä oikeuksia kuitenkin rajoitetaan useiden ohjelmaryhmien kohdalla. Kaikille sovellusohjelmille annetaan pelkästään suoritusoikeudet, mutta scripteille ja ajonaikaisille kirjastoille asetetaan myös lukuoikeudet. Lukuoikeudet on annettava siksi että jotkut ohjelmat tutkivat kirjaston olemassaoloa yrittämällä lukea sitä. Sovellusohjelmien erityistapauksena ovat ohjelmat, joilla voi tehdä verkkoyhteyksiä Windowsin DOS-ikkunasta, näiden ohjelmien käyttäminen estetään poistamalla niiltä kaikki oikeudet.

DeskTop:n omille konfiguraatiotiedostoille, Windowsin systeemin konfiguraatiotiedostoille sekä MSDOS:n käynnistyistiedostoille asetetaan vain lukuoikeudet, joten kukaan ei pääse niitä muuttamaan.

Windowsin systeemihakemistolle asetetaan luku- ja suoritusoikeudet, ja levykeasemalle asetetaan luku-, kirjoitus,- ja tuhoamisoikeudet mutta estetään ohjelmien ajaminen sieltä. Lisäksi estetään myös että ohjelmien kopiointi sellaisiin hakemistoihin, joissa olevat tiedostot saavat suoritusoikeuksia. Näin ylläpito voi estää käyttäjiä asentamasta omia hyväksymättömiä ohjelmiaan järjestelmään. Asennetut oikeudet myös estävät käyttäjiä kopioimasta ohjelmia pois järjestelmästä.

### *Privileged programs*

Windowsia ei ole suunniteltu sisältämään tiedosto-oikeuksia, ja on olemassa joukko ohjelmia, jotka eivät tule toimeen tiedosto-oikeuksien kanssa. Toisaalta on olemassa myös ohjelmia joiden on pystyttävä tekemään työnsä riippumatta asetetuista oikeuksista. Sellaisia ohjelmia ovat erilaiset asennusohjelmat, muut systeemien hallintaan tarkoitetut ohjelmat (esim. Microsoft system management) tai ohjelmat, jotka toimiakseen tarvitsevat jostain syystä oikeuksia joka paikkaan.

Jotta DeskTop pystyisi toimimaan myös näiden ohjelmien kanssa tai että se olisi edes mahdollista, vaikka se aiheuttaisikin turvallisuusaukon (Asiakkaalla on jokin sovellus, jonka on ihan pakko toimia.), on DeskTop:issa mahdollista määritellä etuoikeutettuja ohjelmia (Privileged programs). Nämä ohjelmat luetellaan siten, että niiden koko polku on näkyvissä, (Esimerkiksi c:\windows\install.exe) ja DeskTop sallii näiden ohjelmien ohittaa tiedosto-oikeudet.

Tietyt ohjelmat vaativat vielä että ne on käynnistettävä taustalla ja mielellään ennen varsinaista Windows:in käynnistämistä. Myös näille on DeskTop:ssa olemassa oma ryhmänsä: Privileged backround programs.

## 5.2.5. Auditointi

Auditointia tarvitaan jotta pystytään selvittämään jälkikäteen mitä järjestelmässä on tapahtunut: kuka on tehnyt mitä ja milloin? Auditoinin kohdalla on hyvin oleellista myös se, että auditointi-informaatiota ei pystytä väärentämään, poistamaan tai muuttamaan. Ainakaan ilman että siitä jää jokin jälki. Auditointia varten voi olla olemassa jokin tietty käyttäjätunnus tai ryhmä. Edes ylläpitäjät eivät välttämättä pysty tutkimaan auditointilokeja.

### *Auditointi ja verkkokäyttöjärjestelmä*

Sekä Microsoft:n että Novell:n verkkokäyttöjärjestelmissä on olemassa auditointi-järjestelmät, jotka käsittelevät verkkokäyttöjärjestelmään liittyviä tapahtumia. Näitä tapahtumia ovat esimerkiksi uuden käyttäjän luominen, vanhan käyttäjän poistaminen, käyttäjäryhmän luominen, tiedosto-oikeuksien muuttaminen ja erilaiset informatiiviset ilmoitukset kuten virheiden reportointi.

NetWare:ssa on olemassa erillinen auditoija-tunnus auditointia varten. NT:ssä puolestaan tavallisesti ylläpitäjä toimii myös auditoijana.

### *Auditointi ja DeskTop*

Verkkokäyttöjärjestelmän auditointi ei ulotu itse työasemaan. DeskTopilla voidaan auditoida myös työasemaa. Auditointintia varten luodaan TWD_AUDITORS ryhmä, jonka jäsenet toimivat auditoijina. Näillä henkilöillä on oikeus valita mitä auditoidaan ja tutkia audit-lokeja.

*Audit-loki on tiedosto, johon tulee merkintöjä järjestelmässä tapahtuneista tapautumista. Se tulee olla suojattu ja sitä ei saa päästä muuttamaan järjestelmän ulkopuolelta.*

Auditoinissa ongelmatilanteen muodostaa se mitä tehdä kun lokitiedosto tulee täyteen. Jos tiedoston annetaan rajattomasti kasvaa, se täyttää ennemmin tai myöhemmin koko kovalevyn ja estää tietokoneen käyttämisen. Toimintavaihtoehtoja tiedoston täyttyessä on useita: auditointi voi yksinkertaisesti loppua kun uusia merkintöjä ei pystytä enää tekemään. Toinen vaihtoehto on, että ei sallita työaseman käyttämistä auditlokin

täytyttyä, vaan vaaditaan, että auditoijan on tällöin tultava tyhjentämään loki. Kolmas vaihtoehto on, että lokitiedostoja kopioidaan automaattisesti jonnekin ennalta määrättyyn paikkaan. Sieltä auditoija voi niitä tarkastella ja tarvittaessa vapauttaa levytilaa tuhoamalla vanhoja lokitiedostoja. Neljäs vaihtoehto on, että loki on ns. kiertävä lokitiedosto: kun tiedosto tulee täyteen, aletaan kirjottaa vanhojen merkintöjen päälle.

*DeskTop:ssa auditointi lokitiedosto tehdään työasemaan. Tiedoston maksimikoko on säädettävissä. Tiedosto on kiertävä loki. Lokitiedostot voidaan myös halutessa kopioida automaattisesti palvelimelle, josta niitä voidaan tutkia ilman että auditoijan on käytettävä juuri sitä tietokonetta, jota hän haluaa auditoida.*

DeskTop:n käynnistyessä se avaa auditlokitiedoston ja pitää sitä varattuna. Samalla se varmistaa ettei mikään muu sovellus pysty käsittelemään sitä.

Audit lokimerkintöjen rakenne on sama kuin ITSEC:in vaatimuksissa.

## *Auditoinin kohteet*

Auditoija pystyy valitsemaan mitä kaikkea hän haluaa auditoitavan. Aina ei ole toivottavaa auditoida kaikkia mahdollisia tapahtumia, sillä tiedon määrä kasvaa hyvin nopeasti ja oleellinen tieto hukkuu helposti tietotulvaan.

Valittavia auditoininkohteita ovat:

- Login ja Logout, merkintä tulee aina kun käyttäjä joko kirjottautuu järjestelmään tai poistuu sieltä.
- Lock ja Unlock, auditlokimerkintä tulee aina kun näytönsäästäjän lukko menee päälle tai pois päältä. Unlock:ssa voi myös käyttäjätunnus vaihtua.
- Fileaccess violations, tiedosto-oikeuksien rikkominen. Merkintä tulee aina kun ohjelma rikkoo tehtyjä tietosto-oikeus-määrittelyjä.
- Network connections, verkkoyhteyksien muodostaminen. Aina kun käyttäjä muodostaa uuden verkkoyhteyden, siitä jää merkintä.
- Starting programs, ohjelmien käynnistäminen. Jokaisesta käynnistetystä ohjelmasta jää merkintä.
- DeskTop profiilien tallentaminen. Käyttäjien tai ylläpitäjien tekemistä työpöytien konfiguraatioiden tallentamisesta tehdään merkintä.

- Turvallisuusasetusten muokkaaminen. Ylläpitäjän muuttaessa turvallisuusasetuksia tehdään lokimerkintä.

- DeskTop:n virhetilanteet ja virheiden tiedot voidaan myös tallentaa. Näin voidaan jälkeenpäin tutkia mikä on mennyt vikaan.

Ylläpitäjillä voi olla tarve auditoida tiettyjen kriittisten sovellusten käyttöä, sillä kaikkien levyoperaatioiden auditointi on liian raskasta ja suorituskyvyllisesti ongelmallista. Sen sijaan voisi olla käyttökelpoista, jos voisi määrittää haluttujen sovelluksien auditoinin. Tälläinen määrittely voisi olla esimerkiksi osana tiedosto-oikeuksien määrittelyä.

### 5.2.6. Windowsin rajoitukset

Windowsilla on myös paljon omia asetuksia jotka vaikuttavat monenlaisiin asioihin. Käyttäjä voi määritellä Windowsin ulkonäköä koskevia tekijöitä ja millaisia laitteita työasemaan on kiinnitetty.

***Ohjauspaneli***

Suurin osa Windowsin konfiguraatioon vaikuttavista ohjelmista on koottu samaan paikkaan. Tätä konfiguraatiotyökalujen käynnistysalustana olevaa työkalua kutsutaan ohjauspaneliksi. Ohjauspanelista voidaan säätää mm seuraavia asioita: Windowsin värejä, aikaa ja päivämääriä, työpöydän taustamateriaalia, näytönsäästäjää, fontteja, kansallisia asetuksia, näppäimistön ja hiiren asetuksia, kommunikointiporttien asetuksia, virtuaalimuistin asetuksia, käytettyjä verkkoprotokollia, verkkokortteja ja niiden ajureita sekä printtereitä ja ääniasetuksia.

Monet näistä asetuksista ovat sellaisia, joiden käyttäjien muuttamismahdollisuuksia ylläpitäjät haluavat kontrolloida. Verkkokortin asetusten virheellinen muuttaminen muun muassa estää koneen pääsyn palvelimelle ja työaseman käyttämisen. Samoin ei ole yleensä suotavaa, että käyttäjät muuttavat virtuaalimuistin asetuksia.

DeskTop:lla on mahdollista valita mitä näistä ryhmistä käyttäjät voivat muuttaa. Ylläpitäjä voi luetella ne ryhmät, joiden käyttäminen estetään käyttäjältä jolloin käyttäjät eivät pysty käynnistämään kyseisiä konfiguraatiotyökaluja. Samalla kyseisten työkalujen ikonit katoavat käyttäjien näytöltä.

### *Verkkoresurssit ja niiden jakaminen*

Konfiguraatioon vaikuttavien ohjelmien lisäksi ylläpitäjät voivat määrittää muita yleisiä asetuksia, jotka vaikuttavat työaseman turvallisuuteen. Yksi tälläinen asetus on Windows:n sammuttaminen. Jos Windowsin sammuttaminen on sallitua käyttäjille, he voivat poistua Windowsista takaisin DOS:iin ja samalla ohittaa kaikki DeskTop:n turvallisuusasetukset. Yleensä tämä ei ole sallittua muille kuin ylläpitäjille.

Windows työasemasta on myös mahdollista jakaa resursseja siten, että ne näkyvät työaseman ulkopuolelle. Mikäli tämä sallitaan pystyy käyttäjä jakamaan koko kiintolevynsä verkkoon ja käyttämään toista työasemaa ja käyttämällä toista työasemaa ohittamaan tiedosto-oikeus-määrittelyjä. *DeskTop:ssa on mahdollista kieltää sekä omien resurssien jakaminen ulospäin että uusien verkkoyhteyksien luominen.*

### *Program Manager*

Windowsin yleisimpänä käyttöliittymänä toimii Program Manager-niminen ohjelma. Siitä käyttäjät pystyvät käynnistämään uusia ohjelmia. Unix-maailmassa Program Manager vastaisi lähinnä shelliä. Program Managerin käynnistäminen ei ole pakollista, ja sen tilalla voikin toimia jokin muu ohjelma. Jos halutaan käyttää Windowsia vain yhden sovelluksen ajamiseen, silloin korvataan Program Manager tällä ohjelmalla.

DeskTop:lla voidaan asettaa turvallisuusasetuksia myös Program Manageriin. Ylläpitäjät voivat päättää, onko Program Managerin käynnistäminen yleensäkään sallitua. Program Managerin menu-komennoissa on muun muassa "aja" komento, jossa käyttäjä voi antaa suoraan sen ohjelman nimen ja polun, jonka hän haluaa suoritettavan. Tämä komento on mahdollista kieltää.

Program Manager tallettaa aina tietoja omista ikkunoistaa, ikoneistaan ja ohjelma-ryhmistään. Ylläpitäjät voivat vaikuttaa myös siihen, mitkä operaatiot ovat sallittuja ja siihen, tallennetaanko muutoksia.

Haluttaessa voidaan rakentaa järjestelmä, jossa käyttäjälle kaikki näyttää aina samanlaiselta ja löytyy samoilta paikoilta. Samalla myös estetään käyttäjän tahaton asetuksien muuttaminen. Yleisessä tapauksessa käyttäjät tietysti haluavat muuttaa asetuksia ja niiden muuttaminen tietyissä rajoissa on sallittua. Rajan asettaa yleensä se, vaikuttaako asetus turvallisuusominaisuuksiin.

## 5.2.7. Resurssiobjektien uudelleenkäyttäminen

Resurssiobjektien uudelleenkäyttämisen vaatimus periaatteessa tarkoittaa, että kaikki objektit, jotka käyttöjärjestelmä saa takaisin sovelluksilta, nollataan ennen kuin ne annetaan uudelleen käytettäviksi. Objekteja ovat kaikki erilaiset muistiobjektit ja pinot sekä kaikki levyllä olevat tiedostot.

Yhden käyttäjän järjestelmissä objektien uudelleenkäyttämisen aiheuttama turvallisuusriski on luonnollisesti pienempi kuin järjestelmissä, joissa voi olla samaan aikaan useita käyttäjiä.

Kaikkien tiedostojen nollaaminen aina kun ne vapautuvat on melkoinen suorituskykyongelma ja näin ollen se olisi käytännössä käyttökelvoton. Sen sijaan voitaisiin määrittää tiedostoja ja villikorttimäärittelyjä tiedostoista, jotka poistuessaan tyhjennettäisiin. Valitettavasti aikataulut eivät sallineet tämän toteuttamista.

*DeskTop:ssa voi määrittää tiedostoja ja hakemistoja, jotka tuhotaan aina kun käyttäjä poistuu järjestelmästä tai kun käyttäjä kirjottautuu sisään järjestelmään. Tuhoaminen tehdään molemmissa tapauksissa siksi, että tiedostot tuhotaan myös siinä tapauksessa että tietokone on uudelleen käynnistetty resetoimalla se tai katkaisemalla sähköt.*

## 5.2.8. Erikoiset ohjelmaryhmät

DeskTop:ssa voidaan määrittää ohjelmia joilla on erityisiä ominaisuuksia verrattuna muihin ohjelmiin. Tiedosto-oikeuksien yhteydessä on jo mainittu etuoikeutetut ohjelmat, jotka pystyvät ohittamaan tiedosto-oikeus määrittelyt.

### *Taustalle käynnistettävät ohjelmat (Backround programs)*

Taustalle käynnistettävät ohjelmat käynnistetään automaattisesti kun käyttäjä kirjottautuu sisään. Ohjelmat ilmestyvät minimoituna ruudulle. Taustalle käynnistettävät ohjelmat käynnistetään ennen varsinaista DeskTop:n käynnistämistä. Näitä ohjelmia ei myöskään sammuteta käyttäjän poistuessa. (Tietenkin sillä edellytyksellä että Windows jää kuitenkin päälle.) Tälläisiä ohjelmia ovat esimerkiksi jotkin spoolerit, joiden pitää olla kokoajan käynnissä.

DeskTop:lla on itsellään käytössä yksi taustalla toimiva ohjelma; tmlogon.exe. Tämän ohjelman tehtävänä on tarjota automaattisia sisäänkirjottautumis palveluita ja keskustella tarvittaessa TeamOfficen automaattisen saapuneesta postista tiedoittavan ohjelman kanssa (TeamAlarm). TeamAlarm pitää yhteyttä postipalvelimeen myös silloin kun

käyttäjä ei varsinaisesti ole kirjottautunut sisään postipalvelimeen. DeskTop pitää huolta, että tämä yhteys on asetettu aina oikealle käyttäjälle, ja käyttäjän kirjottautuessa ulos DeskTop:sta tmlogon.exe kirjottaa käyttäjän ulos myös TeamOfficesta.

### *Etuoikeutetut taustalle käynnistettävät ohjelmat (Privileged backround programs)*

Myös tähän ryhmään kuuluvat ohjelmat käynnistetään aina sisäänkirjottautumisen yhteydessä. Lisäksi ne pystyvät ohittamaan tiedosto-oikeudet. Ryhmään kuuluvat ohjelmat on määriteltävä kokonaan polkuineen.

### *Ensimmäiseksi sammutettavat ohjelmat (Terminate first)*

Windowsia sammutettaessa ensimmäiseksi sammutettavien ohjelmien ryhmään kuuluvat ohjelmat sammutetaan ennen muita ohjelmia. Joidenkin ohjelmien on oltava suljettuina ennenkuin Windows voidaan sammuttaa.

### *Single instance*

Single instance ohjelmia voi olla käynnissä vain yksi kappale. Jos käyttäjä yrittää käynnistää toista kopiota samasta ohjelmasta, se estetään.

### *Automaattisesti pienennettävät ohjelmat*

Automaattisesti pienennettävien ohjelmien ryhmään kuuluvat ohjelmat minimoidaan aina kun näytönsäästäjä-lukko menee päälle. Tämä toiminnallisuus on rakennettu lähinnä TeamOffice ohjelmia silmällä pitäen. TeamOffice ohjelmat katkaisevat yhteyden palvelimeen, kun ne pienennetään. Tällöin palvelimen kuorma pienenee, kun yhteydet jotka eivät ole aktiivisia sammutetaan.

## 5.3. DeskTop ja Konfiguraationhallinta

DeskTop:n yhtenä tavoitteena oli tarjota ympäristö, jossa ylläpitäjät voivat helposti ja tehokkaasti hallita laajoja työasemaverkkoja ja jossa käyttäjät pystyvät jakamaan työasemia. Molempien vaatimuksien toteuttaminen vaatii, että on olemassa, jokin mekanismi jolla voidaan jakaa ja hallita konfiguraatiotietoja keskitetysti. Ylläpitäjien työmäärä helpottuu oleellisesti jos he voivat hallita useampia työasemia samasta paikasta, eikä heidän tarvitse olla aina läsnä siinä paikassa, jonka työaseman konfiguraatioon he haluavat tehdä muutoksia. Käyttäjät puolestaan haluavat säilyttää omat asetuksensa eri työasemissa, ja samaa työasemaa voi käyttää useampi kuin yksi henkilö.

*Konfiguraatio määriteltiin käsittämään kaikki se tieto, joka määrää miten Windows ja siihen asennetut ohjelmat toimivat.*

DeskTop:ssa voidaan määrittää erilaisia konfiguraatioita, niitä voidaan keskitetysti ja ne voidaan tehokkaasti jakaa eri työasemien välillä.

DeskTop kokoaa Windowsin konfiguraation käynnistyksen yhteydessä sen mukaan, miten ylläpitäjät ovat konfiguraationhallinnan järjestäneet.

Ylläpitäjät määrittävät mitä osaa konfiguraatiosta hallitaan. He päättävät mitä mahdollisuuksia käyttäjillä on vaikuttaa Windows ympäristöönsä. Käyttäjät saavat tehdä muutoksia konfiguraatioon vain niiltä osilta, minkä ylläpitäjät ovat sallinneet.

Ylläpitäjillä on myös mahdollisuus määritellä konfiguraatio tieto kuulumaan konfiguraationhallinnan ulkopuolelle. Tällöin ko. konfiguraatioasetukset käyttäytyvät samalla tavalla kuin jos DeskTop:a ei olisi työasemaan asennettukaan.

Konfiguraatiot ovat monimutkaisia kokonaisuuksia, ja erilaiset asetukset saattavat yllättävästi vaikuttaa toisiinsa. Ylläpitäjien täytyy olla varsin hyvin perillä ohjelmien tavasta säilyttää tietoaan pystyäkseen kokoamaan yhtenäisen ja helposti hallittavan kokonaisuuden. DeskTop säilyttää tietoa kootusti samassa paikassa, mikä mahdollistaa helpomman ylläpitämisen, mutta samalla epästabiilin konfiguraation vaikutus kasvaa. Ylläpitäjä voi vahingossa yhdellä komennolla saada kaikki työasemat toiminta-kyvyttömään tilaan.

## 5.3.1.Konfiguraationhallinnan hierarkia

Konfiguraatiotietoa on hyvin monenlaista ja kaikkia asetuksia ei kannata eikä myöskään voi siirtää eri työasemien välillä. Varsin monet eri asetukset ovat yhteisiä eri käyttäjien kesken, joten olisi mielekästä ettei samoja asetuksia tarvitsisi määritellä useisiin paikkoihin.

### *Konfiguroinin kohteet*

Erilaisia konfiguraatiotiedostoja on olemassa lukematon määrä. Tiedoston sisältö, tyyppi (esim. tekstitiedosto, binääritiedosto) ja rakenne voi olla mielivaltainen. Yleensä ei ole mahdollista tulkita tiedoston sisältämää tietoa. Mielivaltaista konfiguraatiotiedostoa joudutaan käsittelemään kokonaisena tiedostona.

Erikoistapauksen muodostavat juuri ini-päätteiset tiedostot. Niiden rakenne on määritelty ja DeskTop sallii niiden käsittelemisen yksityiskohtaisemmalla tasolla. Ini-tiedosto jakautuu osioihin (sektio). Osioissa on puolestaan tekstimuotoisia rivejä, joilla kullakin on avain ja arvo.

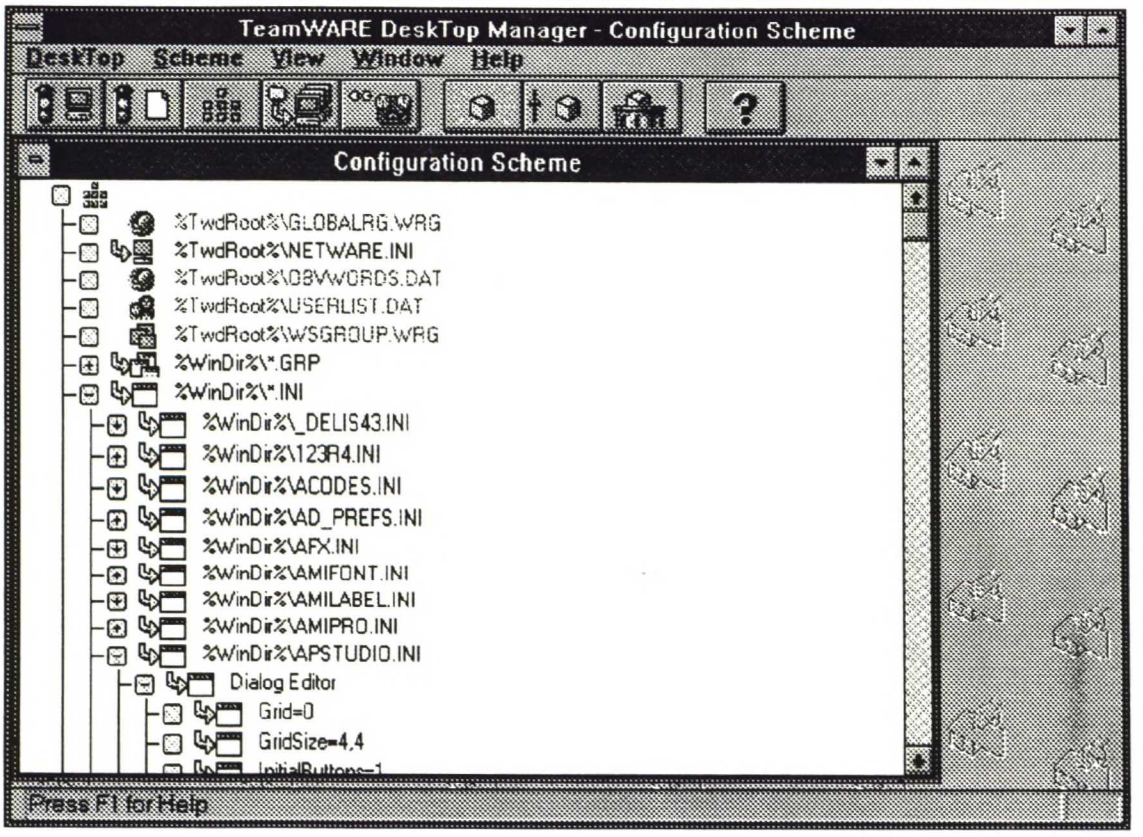
DeskTop:ssa konfigurointi voidaan kohdistaa kuhunkin näistä tasoista (tiedosto, osio ja avain). Kuvassa 4 näkyy kuinka DeskTop esittää konfiguraatiota ylläpitäjälle. Kuvassa on selattu auki erästä konfigurointia. Ylläpitäjä voi hiirellä selata konfiguraatiotietoja ruudulla ja tarvittaessa tehdä haluamiaan muutoksia.

Tässä konfiguroinin esittämishierarkiassa alemmalla tasolla oleva asetus on aina ylemmän tason mukainen, jollei muuta ole erikseen sanottu.

### *Konfiguraatiotiedoston nimeäminen DeskTop:ssa*

DeskTop sallii että, tiedoston nimessä on mahdollista käyttää villejä kortteja (wild cards) ja ympäristömuuttujia. Villikorteilla on mahdollista muodostaa tiedostoryhmiä. Esimerkiksi c:\windows*.ini määrittelisi kaikki kyseisessä hakemistossa olevan ini-päätteiset tiedostot. Ympäristömuuttujia voidaan määritellä autoexec.bat:ssa ennen Windowsin käynnistymistä. Yksi käytetty ympäristömuuttuja on nimeltään WinDir. WinDir osoittaa siihen hakemistoon, johon Windows on installoitu. Esimerkissä mainitut c:\windows hakemistossa oleviin ini-tiedostoihin voidaan siis yleisessä tapauksessa viitata %WinDir%*.ini. Tällöin ei ole merkitystä minne Windows itseasiassa on asennettuna.

Konfigurointia voidaan kohdistaa myös villikorteilla ja ympäristömuuttujilla osoitettuihin konfiguroinin kohteisiin.




Kuva 5.

## *Konfiguroinin tasot*

*Konfiguroinin tasoilla tarkoitetaan niitä tasoja, joihin konfiguraatiotieto voidaan luokitella. DeskTop jakaa konfiguraatiotiedot seitsämälle eri tasolle.*

Kuvassa 5 on esitettynä kaikki tasot ja miten ne muodostavat hierarkian. (Kuva on DeskTop:n ylläpitäjän-työkalusta. Kuvassa olevalla ikkunalla ylläpitäjä voi tehdä muutoksia konfiguroinin kohteeseen.

1. Globaali taso: Globaalilla tasolla olevat asetukset ovat yhteisiä kaikille työpöydille kussakin ympäristössä. Kaikki käyttäjät, tietokoneet ja ryhmät jakavat nämä asetukset samanlaisina. Globaaleja asetuksia hallitaan keskitetysti samasta paikasta, ja ne voidaan haluttaessa kopioida yritystason verkoissa eri DeskTop ryhmiin.

Seuraavat kolme tasoa muodostavat kokonaisuuksia kolmella eri suunnalla.

2. Työpöytäryhmä (Group Desktop): Asetus on yhteinen kaikille saman verkkokäyttöjärjestelmän ryhmän jäsenille. Samaan ryhmään kuuluvilla käyttäjillä on tyypillisesti käytössään samoja ohjelmistoja. Esimerkiksi näille ohjelmille kuuluvat ei-käyttäjäkohtaiset asetukset kuuluvat tähän ryhmään.

3. Kaikki käyttäjät (All Users): Tämän asetuksen jakavat kaikki käyttäjät. Riippumatta siitä mihin ryhmään käyttäjät kuuluvat tai mitä tietokonetta he käyttävät, asetus on heille yhteinen.

4. Työasemaryhmä (Workstation Group): Asetukset ovat yhteisiä kaikille samaan työasemaryhmään kuuluville tietokoneille. Tietokoneet jaetaan työasemaryhmiin DeskTopin asennuksen yhteydessä. Samalle työasemaryhmälle on tyypillistä yhtenevä laitteistokonfiguraatio ja sijainti.

Viimeiset kolme tasoa kohdistuvat yksittäisiin kohtaisiin.

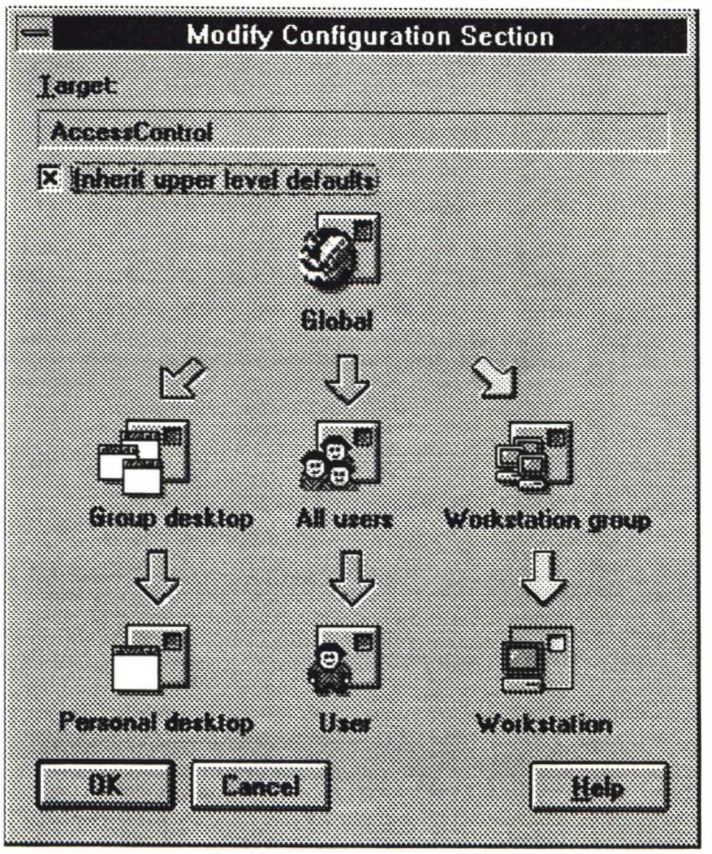
5. Käyttäjä: Asetus on henkilökohtainen käyttäjälle. Jokaisella käyttäjällä kyseinen asetus on erilainen. Olipa valittu työpöytä mikä hyvänsä, asetus on sama. Tälläisia asetuksia ovat esimerkiksi käyttäjän nimi (kaikilla yleensä erilainen ja sama huolimatta käytetystä työpöydästä) ja sähköpostitunnus.

6. Henkilökohtainen työpöytä: Asetus on määritelty seuraamaan kyseisen käyttäjän tiettyä työpöytää. Näitä asetuksia ovat esimerkiksi käyttäjän ko. työpöydälle asentamat omat ohjelmat, näiden ohjelmien konfiguraatitiedot sekä ikkunoiden paikat ja koot. Saman käyttäjän eri työpöydillä nämä asetukset ovat erikseen määriteltävissä ja ne voivat olla erilaisia.

7. Työasema: Työasemakohtainen asetus on erikseen määritelty jokaisessa tietokoneessa ja se voi olla erilainen. Näitä asetuksia ovat kaikki tietokoneen laitteistoihin liittyvät konfiguraatiotiedot. kuten tietokoneessa olevan verkkokortin ja näytönohjaimen ajureiden määrittelyt.

*Työpöydän lataamisella tarkoitetaan palvelimella (tai paikallisessa cachessa) olevien erillisten konfiguroinin osien yhdistämistä niin että muodostuu haluttu konfiguraatio eli työpöytä.*

Riippuen siitä mitä ollaan tekemässä ladataan ja käsitellään eri tasoja. Aina ei suinkaan tarvitse ladata kaikkia tasoja. Lataamisessa voidaan ajatella että kukin konfiguraatio tiedosto kootaan tiedoista mikä on jaettuna näille seitsämälle eri tasolle.




Kuva 6.

### *Periytyminen*

Usein asetuksilla on olemassa jokin mielekäs alkuarvo, jota kuitenkin on pystyttävä myöhemmin muuttamaan. Jokin asetus voi olla yhteinen kaikille käyttäjille kunnes joku käyttäjistä haluaa muuttaa sitä. Käyttäjän tekemä muutos pitäisi säilyä.

*DeskTop:ssa on mahdollista määritellä asetus periytyväksi ylemmältä tasolta. Silloin asetus itse asiassa kuuluu jollekin alemmalle tasolle, mutta niin kauan kun sen arvoa ei ole muutettu, se saa arvonsa ylemmältä tasolta. Mikäli asetuksen arvoa muutetaan se tallettuu määritellylle tasolle ja säilyttää arvonsa.* Kuvassa 6 oleva keltainen nuoli kuvaa asetuksen periytymistä (oikeanpuoleiset nuolet).

Tavallisesti asennuksen yhteydessä suurin osa konfiguraatiotiedoista merkitään periytyväksi globaalilta tasolta. Tiedosto, joka sisältää globaalit määrittelyt on silloin kooltaan suurin - alemmilla tasoilla määritellään vain muutoksia globaalille tasolle.

Sivuvaikutuksena saavutetaan tilansäästöä serverissä, koska samaa informaatiota ei tarvitse tallettaa erikseen useisiin paikkoihin, vaan tieto sijaitsee keskitetysti yhdessä paikassa. Kun työpöytiä käytetään ja muutetaan hitaasti asetuksia siirtyy vähitellen

alemmille tasoille. Ylläpitäjät voivat tarvittaessa myös poistaa käyttäjien tekemät muutokset ja palata takaisin alkutilanteeseen. Alkutilanteeseen palaaminen on erityisen käytännöllistä silloin, kun käyttäjän konfiguraatio on sekoittunut.

Ini-tiedostolla on mahdollista asettaa tasoja myös osioille ja avaimille (section ja entry). Ini-tiedostoilla tapahtuu hieman toisenlaista periytymistä: mikäli konfiguraatioasetus on määriteltynä pelkästään koko ini-tiedostolle, niin määrittely periytyy alemmalle hierarkiatasolle automaattisesti.

***Pysyvät asetukset***

Tietyt asetukset pitää olla määritelty jollekkin tasolle, jotta DeskTop:n ja Windowsin toimiminen olisi mahdollista. Niiden asetusten muuttaminen jollekin toiselle tasolle estäisi Windowsin käynnistymisen. Nämä konfiguraatiotiedot DeskTop on määritellyt pysyviksi, eikä ylläpitäjät voi muuttaa niiden tasoa.

***Konfiguraatiotietojen lisääminen ja poistaminen***

Kaikki konfiguraatiotieto ei ole välttämättä konfiguraationhallinnan piirissä. Konfiguraationhallintaan kuuluvat vain ne tiedostot, jotka siihen on määritelty. Muut konfiguraatiotietoa sisältävät tiedostot toimivat normaalisti, eikä niiden käyttäytymiseen voida DeskTop:n kautta vaikuttaa.

Ylläpitäjät voivat sekä lisätä uusia tiedostoja että poistaa vanhoja tiedostoja konfiguraationhallinnasta.

## 5.3.2. Registry tietokanta

Windows NT:ssä esiteltiin uusi tapa konfiguraatiotietojen tallentamiseen. Sen sijaan että tietoja säilytettäisiin tiedostoissa, ne koottaisiin erilliseen tietokantaan. Käyttöjärjestelmä tarjoaa palveluna funktiot, joilla sovellus ja käyttäjäkohtaista tietoa voidaan tallettaa ja hakea tietokannasta.

Tietokannan etu verrattuna erillisiin tiedostoihin on tietojen helpompi hallittavuus. Kaikki tieto on tallennettuna samaan paikkaan, eikä eri puolille tiedostojärjestelmää. Registryä on mahdollista tutkia RegEdit nimisellä työkalulla.

Registry esiteltiin myöhemmin myös Windows 3.11:een ja myös uusi Windows 95 käyttää sitä. Yhteensopivuussyistä tietoja tallennetaan myös ini-tiedostoihin.

Useat ohjelmat tallentavat asennuksen yhteydessä tietoa registry-tietokantaan. DeskTop havaitsee, että tietokantaa on muutettu ja kysyy ylläpitäjältä, haluaako hän että tehdyt muutokset kopioidaan myös muihin työasemiin. DeskTop näyttää mitä muutoksia ollaan tallentamassa ja ylläpitäjä voi päättää mitä asetuksella tehdään. Vaihtoehtoja ovat 1) asetus kopioidaan toisiin työasemiin 2) asetus kopioidaan toisiin työasemiin vain jos sitä ei siellä jo ole 3) asetusta ei kopioida ollenkaan. Halutessaan ylläpitäjä voi myös muuttaa asetuksen arvoa.

### 5.3.3. Konfiguraationhallinnan toteutus

Konfiguraatiotiedot on jaettuna seitsämälle eri tasolle. Eri tasoilla olevat tiedot ovat tallennettuna palvelimen levylle eri tiedostoihin. Poikkeuksen tähän muodostaa työaseman konfiguraatiotiedot, jotka ovat tallennettuna paikalliseen työasemaan. (työaseman tietoja ei ole mitään hyötyä kopioida verkkoon).

Koska konfiguraatio sijaitsee pienissä erillisissä palasissa eri tiedostoissa, pitää se koota yhteen. Tämä kokoaminen tapahtuu Windowsin käynnistämisen yhteydessä. Työaseman Windows-hakemistoon kootaan kaikki ini-tiedostot. Yksittäisen ini-tiedoston kokoaminen puolestaan tapahtuu parsimalla kyseisen tiedoston sisältö kokoon erillisistä tiedostoista.

Parsimista ohjataan profspec.ini nimisen tiedoston mukaan. Profspec.ini-tiedostoon DeskTop tallentaa tiedot siitä miten konfiguraatio on muodostettu. Profspec.ini:ssä on lueteltuna kaikki tehdyt konfiguraatioasetukset. Asetukset ovat muotoa: konfiguroinin kohde, bittimaski. Konfiguroinin kohde voi olla: tiedostoryhmä, tiedosto, ini-tiedoston osio tai ini-tiedoston avain. Bittimaski kertoo mille tasolle tieto kuuluu, onko tieto periytyvä ja onko tiedoston rakenne sama kuin Windowsin ini-tiedostoilla.

Taulukossa 2 on kuvattuna palvelimen hakemistorakenne. Eri konfiguraation tasoille kuuluvat asetukset on tallennettuna eri tiedostoihin. Eri siteistä ja niissä olevista käyttäjistä tehdään omia alihakemistoja mihin konfiguraatiotiedot tallennetaan.

| |
|---|
| \\PALVELIN\TWD_CONF\ |
| Desktops\ |
| Default.grp |
| Global.def |
| Develope.rs |
| USR\ |
| <SiteName>\ |
| _common_\ |
| <sitename> |
| Käyttäjä1\ |
| Käyttäjä2\ |

Taulukko 2

Ini-tiedosto bittiä tarvitaan silloin kun halutaan käsitellä tiedostoa, joka on ini-tiedosto muotoinen mutta jolla ei ole ini-päätetä.

Profspec.ini on aina määriteltynä kuulumaan ylimmälle tasolle globaaliksi. Jos samassa järjestelmässä käytetään useita sitejä ja useita palvelimia, globaalit asetukset on pidettävä samana. Myös profspec.ini on pidettävänä samana.

Mikäli samaan hakemistopuuhun on asennettuna useampia DeskTop-sitejä, kaikki eri sitet muodostavat oman hakemistopuun haaransa \USR:n alle. Tällöin eri siteillä on omat site-kohtaiset asetuksensa ja käyttäjäkohtaiset asetuksensa, mutta sen sijaan desktop ja globaalit asetukset ovat yhteisiä. Isompaa useita site:jä kattavaa järjestelmää rakennettaessa on mahdollista pitää yhteinen yleinen konfiguraatio kopioimalla yhteiset tiedot eri palvelimiin. DeskTop ei tosin osaa automaattisesti kopioida näitä yhteisiä tiedostoja eri palvelimiin. Tämän toteuttaminen vaatisi palvelin prosessin rakentamista, ja sitä haluttiin välttää.

Taulukossa 3 on esitettynä DeskTopin asennuksessa määriteltävät konfigurointiasetukset

| | |
|---|---|
| %WinDir%*.ini | Ini-tiedosto, periytyvä, käyttäjäkohtainen |
| %WinDir%*.grp | Periytyvä, työpöytäkohtainen |
| %WinDir%\connect.dat | Käyttäjäkohtainen |
| %WinDir%\profspec.ini | Globaali |
| %WinDir%\protocol.ini | Konekohtainen |
| %WinDir%\system.ini | Ini-tiedosto, konekohtainen |
| %WinDir%\deskman.ini | Ini-tiedosto, periytyvä, konekohtainen |
| Deskman.ini UnlockPrivilege-sektio | Periytyvä, käyttäjäkohtainen |
| Deskman.ini DomainSettings-sektio | Periytyvä, sitekohtainen |
| Desktop.ini DesktopConnections-sektio | Työpöytäkohtainen |
| Desktop.ini ConnectionLocations-sektio | Sitekohtainen |
| %WinDir%\tmcrypto.ini | Ini-tiedosto, konekohtainen |

Taulukko 3

### *Sisäänkirjottautumisprosessi*

Sisäänkirjottautuminen ja konfiguraatioiden lataaminen on DeskTop:n yksi monimutkaisimmista ja samalla mielenkiintoisimmista kohdista. Seuraavassa neljässä kuvassa käydään sisäänkirjottautumisprosessi kokonaan läpi.

Sisäänkirjottautuminen alkaa aina käyttäjä tietojen kysymisellä (käyttäjätunnus ja salasana). Jos työasema ei ole lukittuna, käyttäjillä on aina mahdollisuus antaa käyttäjätunnuksensa ja salasanansa. Käyttäjätietojen kysymisen jälkeen tutkitaan onko valittu palvelin olemassa ja saadaanko siihen yhteyttä. Palvelimen olemassa olosta riippuu suoritetaanko sisäänkirjottautuminen paikallisesti vai palvelimelle.

Onnistuneen sisäänkirjottautumisen jälkeen synkronoidaan Global Defaults, työasema, työasemaryhmä ja valitun site:n käyttäjien konfiguraatiotiedot.

*Synkronoinnilla tarkoitetaan, että palvelimella olevat muuttuneet konfiguraatiotiedostot kopioidaan työasemassa olevaan paikalliseen cacheen.*

Konfiguratiotietojen synkronoinin jälkeen siirrytään tarkastelemaan onko työasemakohtainen konfiguraatiotieto mahdollisesti muuttunut DeskTop:n ulkopuolella. Näin käy esimerkiksi siinä tapauksessa, että ylläpitäjä on muuttanut jotain työasemakohtaista tiedostoa DOS:sta. Jos työasemakohtaiset tiedot ovat muuttuneet, talletetaan ne cacheen aina kun se on mahdollista. Tallentaminen ei ole mahdollista, jos edellisen kerran ladattuna ollut konfiguraatio ei ole työaseman tietojen kohdalta täydellinen. Esimerkiksi jos käytössä on ollut pelkkä Global Defaults-työpöytä.

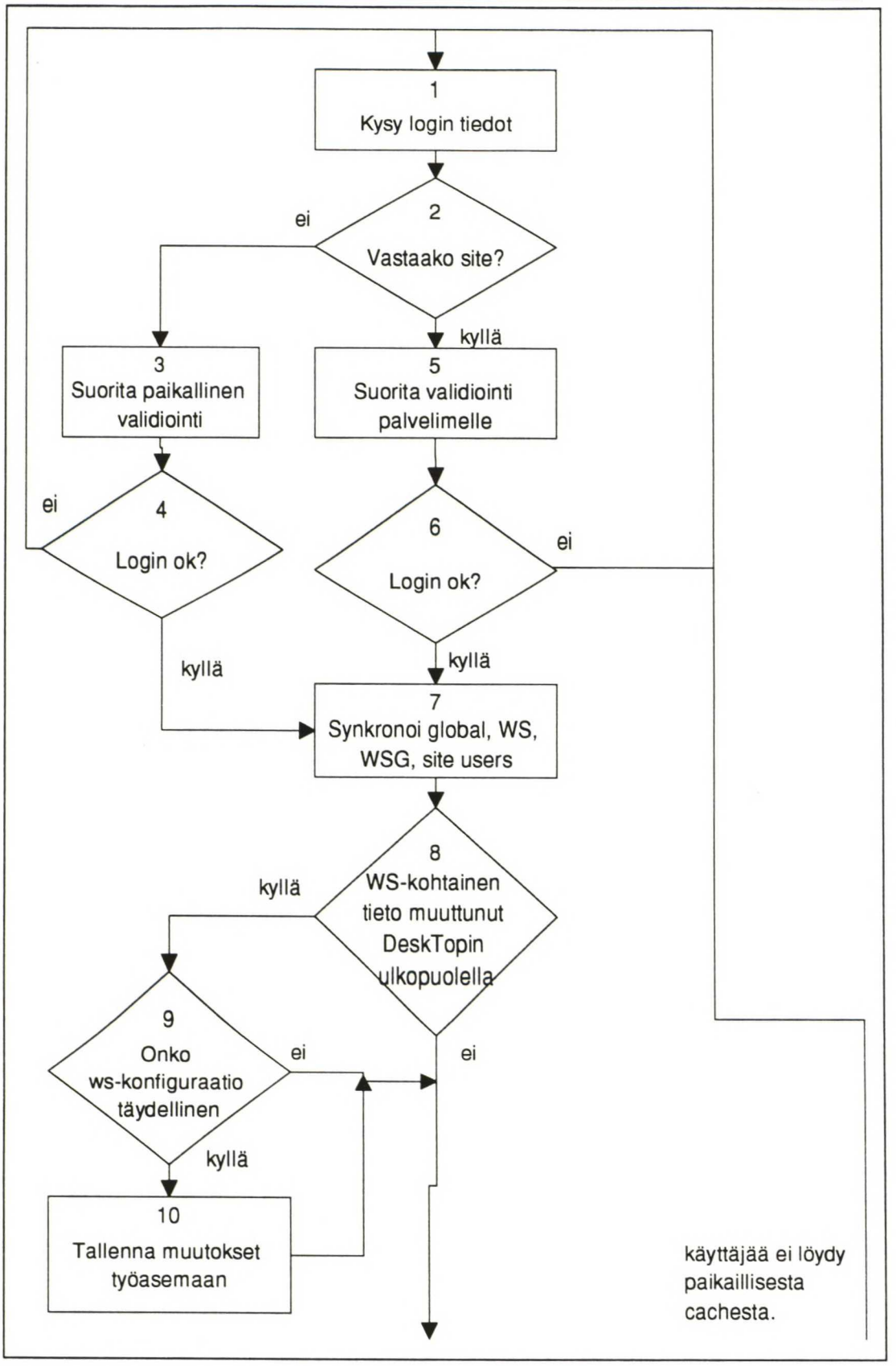
DeskTop:n ulkopuolisten muutosten tarkistamisen jälkeen voidaan siirtyä varsinaiseen konfiguraatin lataamiseen. Lataaminen aloitetaan tarkistamalla onko työasemakohtainen konfiguraatio kunnossa (kuva 8 kohta 11). Jos työasemakohtaisessa konfiguraatiossa on puutteita, se ladataan paikallisesta cachesta.

Työasemakohtaisen konfiguraation käsittelemisen jälkeen sisäänkirjottautuminen jatkuu hieman eritavalla riippuen siitä onko palvelin käytettävissä vai ei. Jos palvelin on käytettävissä tutkitaan onko käyttäjä ylläpitäjä tarkastelemalla kyseisen käyttäjän oikeukssia palvelimella sijaitsevaan wsaccess.tst nimiseen tiedostoon. Jos käyttäjällä on kirjoitusoikeudet ko. tiedostoon hän on DeskTop-ylläpitäjä. Siinä tapauksessa, että palvelin ei ollut käytettävissä, käyttäjän ylläpitäjän oikeudet tarkistetaan paikallisesta tietokannasta. Jos käyttäjää ei tietokannasta löydy, sisäänkirjottautuminen sillä käyttäjätunnuksella on mahdotonta.

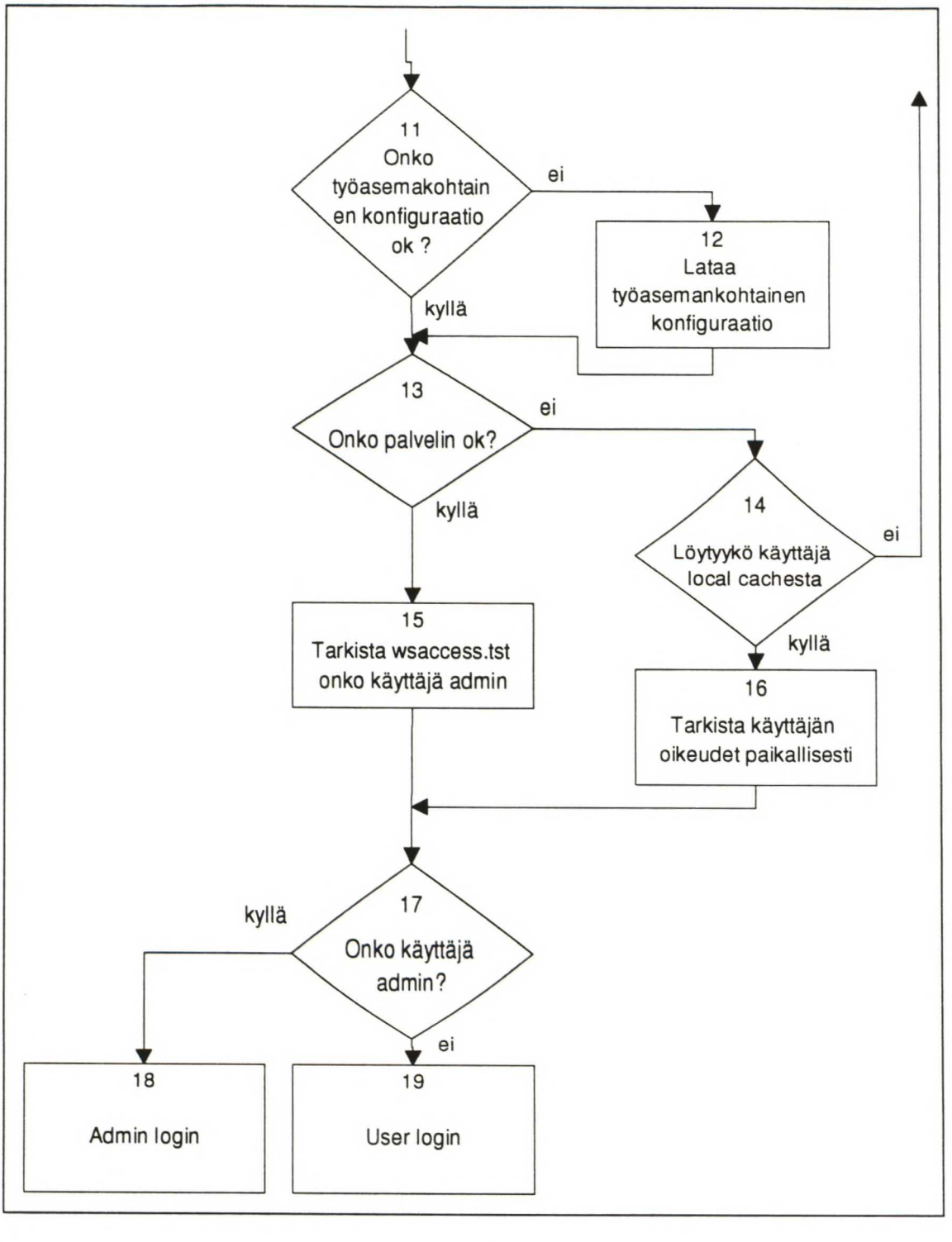
Kuvissa 7 ja 8 on käsiteltynä sisäänkirjottautuminen yksityskohtaisesti tähän saakka. Ylläpitäjän sisäänkirjottautuminen on esitettynä kuvassa 9. Tavallisen käyttäjän sisäänkirjottautuminen on puolestaan käsitelty kuvassa 10.

Kuvissa käytettyjä lyhenteitä:

- WS = workstation, työasema.
- WSG = workstation group, työasemaryhmä
- Global Defaults = Global, globaali taso
- Site users, kaikki siten käyttäjät.
- Admin = ylläpitäjä, User = käyttäjä


1
Kysy login tiedot
2
Vastaako site?
ei
kyllä
3
Suorita paikallinen validiointi
5
Suorita validiointi palvelimelle
4
Login ok?
ei
kyllä
6
Login ok?
ei
kyllä
7
Synkronoi global, WS, WSG, site users
8
WS-kohtainen tieto muuttunut DeskTopin ulkopuolella
kyllä
ei
9
Onko ws-konfiguraatio täydellinen
ei
kyllä
10
Tallenna muutokset työasemaan
käyttäjää ei löydy paikaillisesta cachesta.

Kuva 7

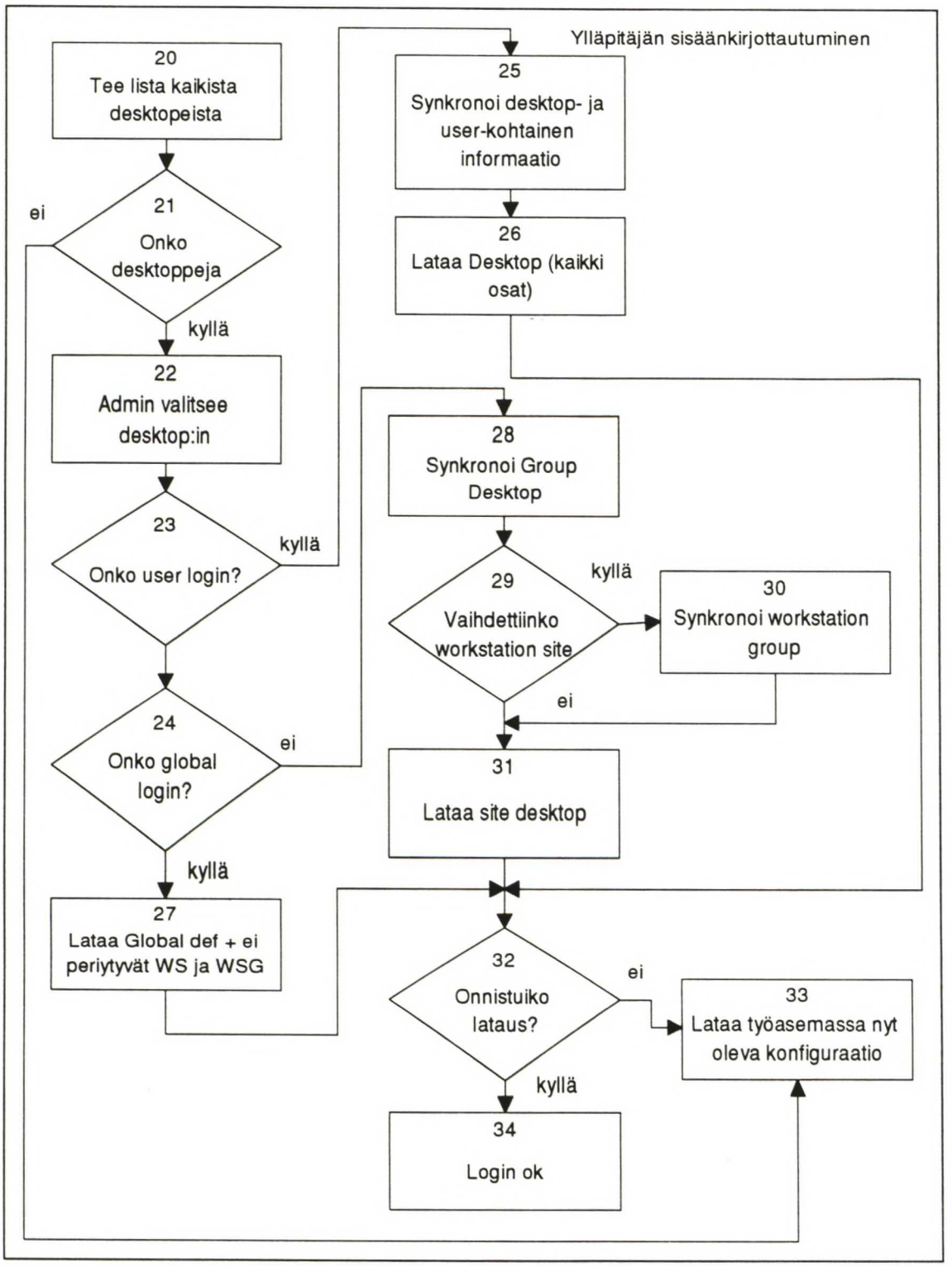



Kuva 8

## *Ylläpitäjien sisäänkirjottautuminen*

Ylläpitäjien sisäänkirjottautumisessa valitaan haluavatko he käyttää työasemaansa tavallisesti vai haluavatko he mahdollisesti konfiguroida jotain työpöytää. Erilaisia tasoja mitä voidaan konfiguroida on useita. Ylimpänä tasona on Global Defaults; työpöytä,

jonkä määrittelemät asetukset ovat yhteisiä kaikille työpöydille. Global Default:n alapuolella on site-taso, site-tason jälkeen tulevat erilaiset työpöydät ja viimeisenä käyttäjien henkilökohtaiset työpöydät.




Kuva 9.

Ylläpitäjä voi tietenkin käyttää DeskTop:a myös tavallisena käyttäjänä, jolloin hänelle on määriteltynä samat turvallisuusvaatimukset kuin muillekkin käyttäjille.

Kuvassa 9 on esiteltynä sisäänkirjottautumisen ja konfiguraation valinnan kulku ylläpitäjän tapauksessa.

Ylläpitäjälle tehdään lista kaikista mahdollisista työpöydistä (kuva 9 kohta 20). Toisin kuin käyttäjillä ylläpitäjän on mahdollista kirjottautua sisään myös silloin kuin työpöytä jostain syystä puuttuu. Tällöin käytetään sitä konfiguraatiota, joka työasemassa sattuu olemaan.

Ylläpitäjä valitseen minkä työpöydän hän haluaa käynnistettäväksi. Valinnasta riippuen tarvittava käyttäjä- ja työpöytäkohtainen informaation synkronoidaan paikalliseen cacheen ja sieltä ladataan Windows-hakemistoon.

Jos ylläpitäjä haluaa konfiguroida jotain tiettyä site-tasoa, hän pystyy vaihtamaan myös työasemasiten. Tällöin myös työasemasitekohtaiset asetukset synkronoidaan ja ladataan.

Jos kaikki tarvittavat osat saatiin ladattua ylläpitäjä pääsee käyttämään valitsemaansa työpöytää. Jos taas jokin osa puuttui tai sitä ei pystytty lataamaan, ylläpitäjä voi kirjottautua sisään siihen konfiguraation, mikä työasemassa sattuu olemaan edellisen käytön jäljiltä.

### *Käyttäjän sisäänkirjoittautuminen ja konfiguraationlataus*

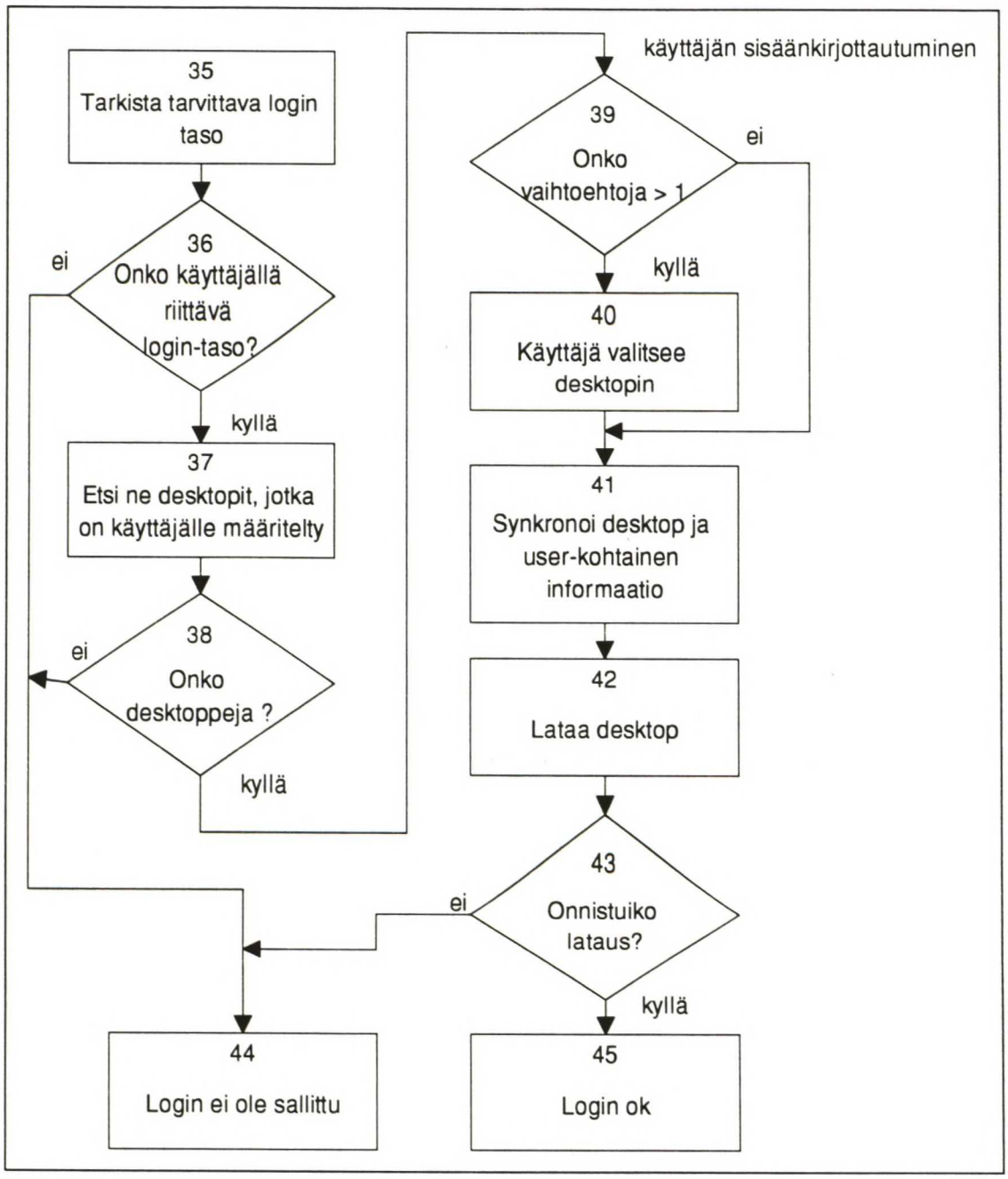
Käyttäjän sisäänkirjottautuminen on yksinkertaisempi kuin ylläpitäjän, koska käyttäjä voi vain käyttää työpöytiään.

Kuvassa 10 on esitetty käyttäjän sisäänkirjottautuminen ja konfiguraationlataaminen.

Käyttäjien kohdalla tarkistetaan onko käyttäjällä riittävä turvallisuustaso sisäänkirjottautumisen tekemiseen. Työasemille on määriteltynä minimiturvallisuustaso, joka vaaditaan.

Turvallisuustason tarkistamisen jälkeen DeskTop muodostaa listan niistä työpöydistä, jotka on käyttäjällä määriteltynä. Jos työpöytiä ei löydy käyttäjän ei ole mahdollista käyttää työasemaa. Jos käyttäjällä on määriteltynä useampia kuin yksi työpöytä, hän valitseen mitä työpöytää hän haluaa käyttää. Käyttäjän tekemän valinnan jälkeen DeskTop synkronoi työpöytä- ja käyttäjäkohtaisen konfiguraationtiedon palvelimen ja paikallisen cachen välillä.

Synkronoinin jälkeen työpöytä ladataan. Latauksessa kootaan konfigurointitiedostot kaikista konfiguraationhallinnan seitsämästä kerroksesta. Samalla tarkistetaan onnistuiko lataaminen. Jos jonkin osa puuttui tai sitä ei pystytty jostain syystä lataamaan. Käyttäjä ei pääse käyttämään työasemaansa. Ainoastaan ylläpitäjien sisäänkirjottautumiset ovat silloin mahdollisia.




Kuva 10

# 5.4. Ohjelmien automaattinen asentaminen

DeskTop mahdollistaa erilaisten ohjelmien ja ohjelmistojen konfiguraatiotietojen siirtämisen työasemasta toiseen. Konfiguraatiotietojen lisäksi täytyy työasemaan tietysti asentaa myös itse ohjelmisto. Usein ohjelmistoja asennetaan verkkopalvelimiin, mutta monesti myös silloin joudutaan kopioimaan joitakin tiedostoja myös työaseman paikalliselle kovalevylle. Toisaalta kaikkia ohjelmia ei pysty asentamaan palvelimelle, vaan ne on asennettava työasemaan. Jos Windows työasemaverkko on laaja, on ohjelmien asentaminen käsin työlästä ja aikaa vievää. Lisäksi jos kyseessä on ohjelman version päivittäminen, voi ongelmia aiheuttaa se, että osassa verkkoa on samaan aikaan käytössä vanha versio, kun muualla jo käytetään uudempaa versiota.

DeskTop:a suunniteltaessa huomattiin, että automaattinen tiedostojen kopiointi työasemien kovalevylle olisi varsin helposti toteutettavissa. Samalla tarjottaisiin yksi ratkaisu helpottamaan ohjelmistojen asentamista. Markkinoilla on olemassa useita työkaluja, jotka ovat erityisesti keskittyneet ohjelmien asennukseen. Esimerkkinä mainittakoon Microsoftin SMS ja TeamWARE Distributor. Varsinaisesti ohjelmien asennus ei kuulu DeskTop:n tärkeimpiin ominaisuuksiin, mutta se täydentää olemassa olevia tuotteita.

## 5.4.1. Rakenne

DeskTop:ssa ohjelmien kopiointi toisiin työasemiin perustuu yhden työaseman hakemistopuun tai puun osan kloonaamiseen toisiin työasemiin. Periaatteena on, että ylläpitäjä määrittelee niin kutsutun kopiointiryhmän (Replication Set), johon kuuluu yksi tai useampia tiedostoja, hakemistopuita tai niiden osia. Kun ryhmä on valmis, se kopioidaan palvelimelle.

Käytännössä uuden kopiointiryhmän luominen tapahtuu siten, että ohjelmisto asennetaan yhteen työasemaan ja siinä työasemassa merkitään mitä tiedostoja pitää kopioida ja minne ne pitää kopioida. Useat ohjelmat haluavat asentaa tiedostoja myös windows- tai system-hakemistoihin. Ylläpitäjän pitää tällöin muistaa merkitä myös nämä ohjelmat kopioitavien ohjelmien joukkoon.

DeskTop olettaa, että kaikissa työasemissa joihin kyseistä kopiointiryhmää ollaan viemässä, on samantyylinen hakemistorakenne. Kopiontiryhmät merkitään kuuluvaksi niihin työasemaryhmiin, joihin tiedostot halutaan kopioida. Työasemaryhmän yhtenä määrittelyperusteena on laitteistokokoonpano, joten samaan ryhmään kuuluvilla

työasemilla on myös samantyylinen hakemistorakenne. Toisaalta mikäli työasemien laitteistorakenne saman työasemaryhmän sisällä on liian erilainen saman kopiointiryhmän käyttämiseksi, voidaan tietysti samasta ohjelmistosta tehdä erilaisia kopiointiryhmiä. Huonona puolena tällöin on se että palvelimella kuluu levytilaa tavallaan turhaan.

Kun käyttäjä seuraavan kerran käynnistää työasemansa ja kirjottautuu sisään palvelimelle, DeskTop huomaa, että kopiointiryhmät ovat muuttuneet, ja kopioi tiedostot paikalliselle kovalevylle.

### *Tilanvaraus*

Eri käyttäjät yleensä käyttävät koneitaan eri tavalla, ja myös vapaana olevaa levytilaa kuluu eri käyttäjillä eri tavalla. DeskTop varmistaa, että paikallisella kovalevyllä on riittävästi tilaa kopiointiryhmien kopioimista varten. Sen se tekee varaamalla levytilaa etukäteen

Työasemaryhmäkohtaisesti määritellään, kuinka paljonko levytilaa varataan. Lisäksi jokaiselle kopiointiryhmälle määritellään kopiointiryhmän tarvitsema tila. Eri kopiointiryhmien yhteenlaskettu levytila on oltava pienempi kuin työasemaryhmälle kopiointia varten kaikenkaikkiaan varattu levytila.

Levytila varataan työaseman kovalevyltä luomalla sinne tarvittavan kokoinen tiedosto. Varatun tiedoston on oltava noin 10% suurempi kuin mitä erillisten tiedostojen yhteenlaskettu tila, koska tiedostojärjestelmästä voidaan varata vain tietynkokoisia paloja kerrallaan. Tästä johtuen paljon pieniä tiedostoja yleensä vie enemmän tilaa kuin tiedostojen yhteenlaskettu koko on.

### *Kopiointi*

Kopioitavia tiedostoja voi olla paljon, ja niiden kopiointi työasemalle voi kestää minuutteja. Koska aina käyttäjän kirjottautuessa sisään työasemaan tarkistetaan se, ovatko kopiointiryhmät muuttuneet, on tarkastus pystyttävä tekemään mahdollisimman nopeasti. Kun kopiointiryhmän tiedostot synkronoidaan (eli kopioidaan uudet tai muuttuneet tiedostot) palvelimelle, DeskTop tekee binäärimuotoisen tiedoston joka sisältää tiedot kopiointiryhmään kuuluvista tiedostoista, niiden koosta ja päiväyksestä. Tarkistukset kopiointiryhmien muutoksista tehdään aina vertaamalla tiedostoja näihin binäärimuotoisiin tiedostoihin.

Jos kopiointiryhmä poistetaan työasemaryhmästä, myös työasemissa olevat tiedostot poistetaan. Käyttäjien käyttäjien kopioitujen tiedostojen joukkoon laittamia omia tiedostoja ei kuitenkaan poisteta.

### *Palvelimen hakemistorakenne*

DeskTop:lla on oma hakemistonsa palvelimella. Kopiointiryhmiä varten tähän hakemistoon luodaan oma alihakemisto. Taulukossa 4 esitellään eräs mahdollinen hakemistorakenne.

| |
|---|
| \\PALVELIN\TWD_CONF\WSREPL\ |
| DEFAULT.INI |
| DEFAULT.DAT |
| DEFAULT\ |
| MSAPPS2.INI |
| MSAPPS2.DAT |
| MSAPPS\ |
| EXCLUDED.INI |

Taulukko 4

Ini-tiedostot sisältävät kopiointiryhmän tiedot. Kopiointiryhmän vaatima koko on tallennettuna samoin kuin tieto siitä ylikirjoitetaanko käyttäjien tekemät omat muutokset, pakataanko tiedostot tilan säästämiseksi, sekä listat ryhmään kuuluvista tiedostoista ja tiedostoryhmistä. Taulukossa 2 olevassa esimerkissä on määriteltynä kaksi kopiontiryhmää: Default ja Msapps. Molemmilla ryhmillä on oma ini-tiedostonsa ja dat-tiedosto.

Usein halutaan kopioida vain osa hakemistopuun tiedostoista. Erityisesti halutaan estää niiden tiedostojen kopioiminen, jotka sisältävät konfiguraationhallinnan piiriin kuuluvaa konfiguraatiotietoa. Tätä varten DeskTop:ssa on erityinen kopiointiryhmä Excluded, johon kuuluvia tiedostoja ei koskaan kopioida minnekään. Näin ylläpitäjä voi määritellä esimerkiksi kaikki winword-hakemistossa olevat tiedostot kopioitavaksi käyttämällä jokerimerkkejä ( c:\winword*.*) ja määritellä tiedostot, joita hän ei halua kopioitavan, kuulumaan excluded-ryhmään.

# 6. Kilpailevat tuotteet

DeskTop:lle ei löydy suoranaisesti kilpailevia tuotteita. Windowsille löytyy kyllä useitakin ohjelmistoja, jotka keskittyvät ohjelmien automaattiseen asentamiseen. Nämä ohjelmat pystyvät tarjoamaan paremman ohjelmien kopioimisen kuin DeskTop, mutta DeskTop:n etuna on se, että se huolehtii myös konfiguroininhallinnasta, ja sen avulla pystytään myös automaattisesti konfiguroimaan ohjelmia eri käyttäjille. Automaattisten asennusohjelmien lisäksi on olemassa koneiden inventointiin tarkoitettuja ohjelmistoja. Näillä ohjelmistoilla saadaan selville käyttössä olevan konekannan laatu ja niihin asennetut ohjelmistot.

## *Salaustuotteet*

Turvallisuustuoteissa kilpailevat tuotteet ovat lähinnä salaustuotteita. Salaustuotteilla voidaan salata tiedostoja ja jopa kokonaisia levyjä ja levyosioita. Usein salaus on totetutettu siten, että käyttäjä ajaa itse jonkin ohjelman, joka tekee salauksen.

Salaaminen vaatii paljon CPU-aikaa ja varsinkin kokonaisten levyjen ja levyosioiden salaamiseen käytetään erillistä tietokonelaitteistoa - esimerkiksi korttia, jolla on salauspiiri. Salauksen merkitys on korostunut - erityisesti kannettavien tietokoneiden osalta, sillä niitähän käytetään myös työpaikan ulkopuolella.

DeskTop itse ei sisällä tietojen salaamista, mutta sitä on mahdollista täydentää TeamWare Cryptolla, jolla saavutetaan tehokas suojaus käyttäjälle läpinäkyvän salauksen kautta. Cryptossa käyttäjä määrittelee mitä hakemistoja tai tiedostotyyppejä käyttäjä haluaa salata. Salauksen määrittely toimii samalla periaatteella kuin DeskTop:n tiedosto-oikeuksien määrittely. Aina kun käyttäjä yrittää jotenkin käyttää salattua tiedostoa, häneltä kysytään tarvittava salasana. Salasanan saatuaan Crypto purkaa tiedoston ja antaa ko. tiedoston käyttäjän saataville. Crypto muistaa annetun salasanan siihen asti kun käyttäjä haluaa lopettaa työskentelyn. Jos kone on käyttämättä kauan, salasana vaaditaan uudelleen. (Aika määräytyy näytönsäästäjän käynnistymisen mukaan.)

Kilpailevia tuotteita pahempi uhka DeskTop:lle ovat uudemmat käyttöjärjestelmät. Jos asiakkaat päättävät siirtyä käyttämään jotain muuta käyttöjärjestelmää, DeskTop:a ei ehkä tarvita.

# 6.1. Kilpailevat käyttöjärjestelmät

Windows 3.1:tä korvaamaan ja sen kanssa kilpailemaan on noussut useitakin uusia käyttöjärjestelmiä. Ne ovat DeskTop:n merkittävimmät kilpailijat, mutta samalla ne osoittavat mihin suuntaan DeskTop:a on kehitettävä.

## 6.1.1. Windows NT

Windows NT on Microsoft:in vastaus Unix-käyttöjärjestelmille. Se on Windows 3.1:teen verrattuna täysin uusi käyttöjärjestelmä, jossa myös turvallisuusominaisuudet on otettu alusta pitäen mukaan suunnitelmiin.

NT:tä suunniteltaessa pyrittiin kiinnittämään huomiota seuraaviin vaatimuksiin /7/.

- Siirrettävyys. Käyttöjärjestelmän piti toimia useissa eri prosessoriarkkitehtuureissa, ja sen sovittaminen uusitte prosessoreille pitää olla mahdollisimman helppoa. Siirrettävyys pyrittiin saavuttamaan kirjoittamalla NT korkean tason ohjelmointikielellä.

- Skaalattavuus ja moniprosessointi. Oletettiin, että tulevaisuudessa käytettävissä olisi enemmän tietokoneita, joissa olisi useita prosessoreita. Samoja sovelluksia pitää pystyä käyttämään sekä yhden prosessorin koneissa että koneissa missä on useita prossoreita.

- Hajautettu laskenta. Tietokoneiden lukumäärän kasvaessa ja niiden välisten verkkojen kehittyessä hajautetun laskennan merkityksen oletettiin kasvavan. Helpottaakseen hajautettua laskentaa hyödynnettävien sovellusten tekemistä, NT:hen rakennettiin hyvä verkkotuki mikä mahdollistaa tehtävän työn jakamisen eri koneiden välillä.

- POSIX-yhteensopivuus. 80-luvun loppupuolella USA:n hallituksen virastot ryhtyivät määrittelemään POSIX-standardia valtion tietokone sovellusten käyttöön. Tarkoituksena oli yhdenmukaistaa valtion käytettävissä olevia tietokonejärjestelmiä. POSIX akronyymi on väljästi määriteltynä "a portable operating system interface based on UNIX". NT:n POSIX yhteensopiivuuden tarkoituksena on helpottaa ohjelmien siirtämistä UNIX-järjestelmistä NT-järjestelmiin. (Microsoft halusi päästä mukaan valtion isoihin kauppoihin.)

- Valtion turvallisuusvaatimusten täyttäminen. USA:n valtio on asettanut omaan käyttöönsä tuleville sovelluksille myös turvallisuusvaatimuksia. NT:n turvallisuustasoksi valittiin C2. NT on myös validioitu tällä tasolla. Tosin validioinnisssa NT:tä käytettiin ilman verkkoa.

Suunnittelun päämääriksi valittiin:

- Laajennettavuus: koodin tulee olla sellainen, että sitä on mahdollista helposti laajentaa ja muuttaa kun vaatimukset muuttuvat.

- Siirrettävyys. Ohjelmat pitää pystyä helposti siirtämään toiseen prosessoriarkki-tehtuuriin

- Luotettavuus ja varmuus (robustness). Järjestelmän pitää suojella itseään sekä sisäisiä virhetilanteita että ulkoisia uhkia vastaan. Sen käyttäytyminen pitää olla ennustettavissa kaikissa tilanteissa, ja sovellusohjelmat eivät saa pystyä vahingoittamaan käyttöjärjestelmää tai sen toimintaa.

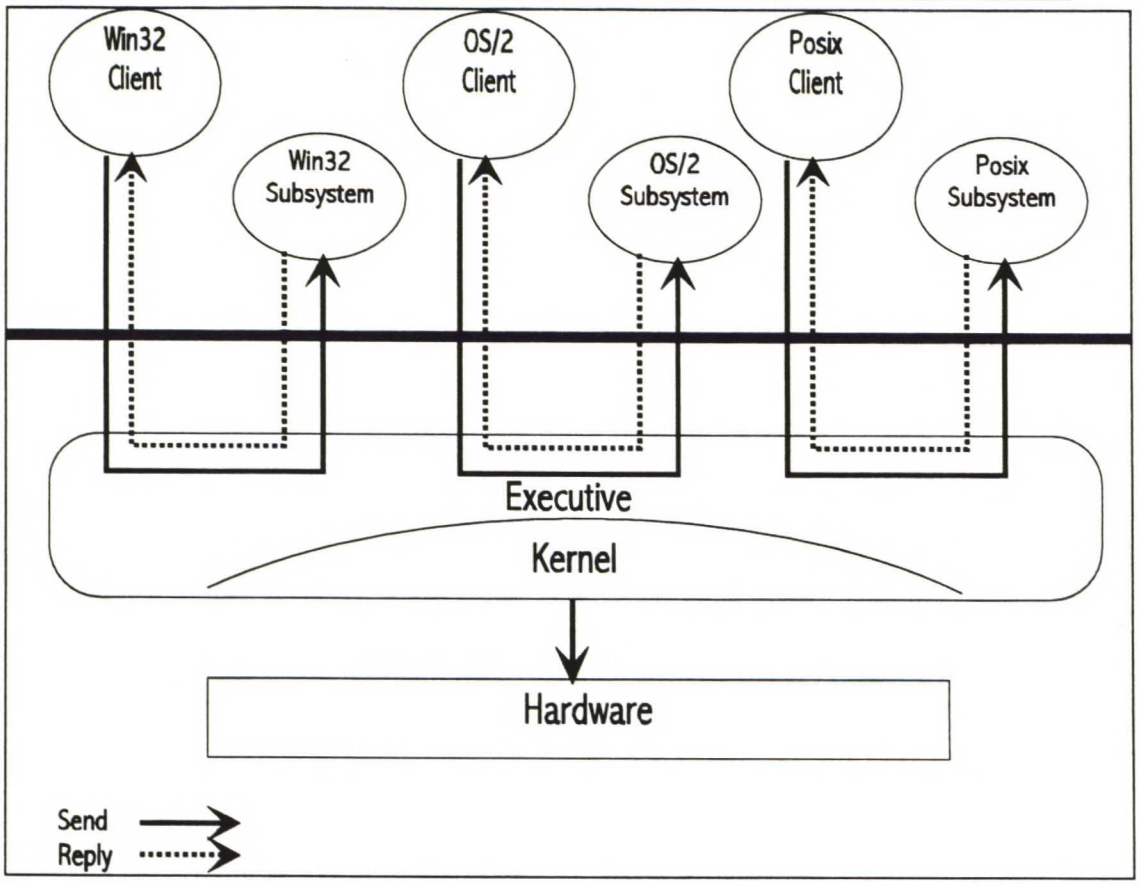
- Yhteensopivuus. Vaikka Windows NT:n tulisi laajentaa olemassa olevaa teknologiaa, sen täytyy olla yhteensopiva olemassa olevien Microsoft:in järjestelmien kanssa.

- Suorituskyky. Muiden suunnitteluvaatimusten lisäksi järjestelmän pitää pystyä toimimaan mahdollisimman nopeasti ja tehokkaasti kaikissa eri arkkitehtuureissa.

## *NT:n rakenne*

NT:n toimita perustuu erilaisiin alijärjestelmiin. Eri alijärjestelmät mahdollistavat erilaisiin järjestelmiin alunperin tehtyjen ohjelmien suorittamisen samaan aikaan samassa koneessa. Samalla se helpottaa ohjelmien siirtämistä muista järjestelmistä NT:hen.

Alijärjestelmät ovat erotettuja ja suojattuja toisistaan, ja yhden alijärjestelmän kaatuminen ei aiheuta muiden alijärjestelmien kaatumista (kuva 11). Koska NT:n varsinainen kerneli on erotettuna alijärjestelmistä, rakenne yksinkertaistuu ja uusien alijärjestelmien tuominen mukaan NT:n rakenteeseen helpottuu.




Kuva 11.

## *NT ja turvallisuus*

Windows NT:n turvallisuusominaisuudet vaativat, että kaikilla käyttäjillä on oltava määriteltynä käyttäjätunnus, ja käyttäjien on sisäänkirjottauduttava koneelle ennenkuin he voivat käyttää konetta. Jokaiselle käyttäjälle on määritelty turvallisuus-profiili, joka on kokoelma turvallisuuteen liittyvää tietoa tallennettuna NT:n järjestelmän tietokantaan. Turvallisuudesta vastaa erityinen oma turvallisuusalijärjestelmä. Turvallisuusalijärjestelmän tehtävänä on varmistaa että käyttäjä on todellakin se kuka väittää olevansa.

Sisäänkirjottautumisen hoitaa turvallisuusalijärjestelmän logon-prosessi. Onnistuneen sisäänkirjottautumisen päätteeksi muodostetaan niin kutsuttu access-token, joka käytetään määrittämään mihin systeemin palveluihin käyttäjällä on oikeudet. Access-token:in luomisen jälkeen turvallisuusalijärjestelmä käynnistää Program Managerin ja kiinnittää siihen kyseisen käyttäjän access-toke:in.

NT tukee useita erilaisia tiedostojärjestelmiä, mutta NT:n omaksi tiedostojärjestelmäksi rakennettiin NTFS (NT-File System) /8/.

NTFS tukee hyvin turvallisuusominaisuuksia. Tiedostoille ja hakemistoille on mahdollista määrittää erilaisia käyttäjä tai käyttäjäryhmä kohtaisia oikeuksia. Oikeuksien määrittämisen lisäksi NTFS on suunniteltu säilyttämään hyvin sisäisen rakenteensa ja toipumaan nopeasti mahdollisista virhetilanteista. (FAT-tiedostojärjestelmän sisäinen rakenne menee sekaisin helposti eikä se osaa korjata itseään automaattisesti. OS/2:seen kehitetty HPFS-tiedostojärjestelmä puolestaan on hyvin hidas toipumaan ongelmatilanteissa.)

NT täyttää ja ylittää DeskTop:in turvallisuusominaisuudet joka suhteessa. Turvallisuuden kannalta DeskTop:n on vaikea tarjota mitään uutta NT:hen. Sensijaan konfiguroininhallinnan puolella DeskTop voi tarjota samoja palveluita työasemalle kuin Windows 3.1:sessäkin. Myös NT:ssä käyttäjien konfigurointitiedot ovat tietokonekohtaisia, ja ne eivät seuraa käyttäjiä tietokoneesta toiseen. Ohjelmat pitää edelleenkin asentaa erikseen eri tietokoneisiin. NT tarjoaa jokaiselle käyttäjälle kyllä oman "työpöydän", mutta samalla käyttäjätunnuksella ei voi olla useita työpöytiä. NT:ssä DeskTop voisikin muotoutua enemmän hallintatuotteeksi kuin turvallisuustuotteeksi.

### 6.1.2. Windows 95

Windows 95 on Microsoft:n uusin käyttöjärjestelmä. Sen tarkoituksena on korvata jo vanhentunut Windows 3.1. Windows 95 tuli markkinoille pitkän odotuksen jälkeen elokuussa 1995. Windows 95 on suunnattu kotikäyttöön, ja sen vaatimukset tietokoneen laitteiston suhteen on suunniteltu sen mukaisesti.

Windows 95 piti poistaa Windows 3.1 rajoitukset ja päästä vihdoin eroon Dosin rajoituksista. Uuden Windowsin myötä on mahdollista siirtyä 32-bittiseen muistiavaruuteen ja unohtaa vanhat segmenttirajoitukset.

Vanhoja Windows-ohjelmia on kuitenkin olemassa niin paljon, että yhtenä tärkeänä suunnittelukriteerinä oli yhteensopivuuden säilyttäminen vanhoihin ohjelmistoihin. Windows 95:n piti pystyä suorittamaan sekä vanhoja 16-bittisiä ohjelmia että uusia 32-bittisiä ohjelmia.

Mahdollisimman suuren yhteensopivuuden säilyttämiseksi, Windows 95 sisältää paljon ohjelmakoodia vanhasta Windows:sta ja ehkä hieman yllättäen Windows 95 onkin paljon lähempää sukua Windows 3.1:lle kuin NT:lle.

### *Windows 95 rakenne*

Windows 95 käyttöjärjestelmän ytimenä toimii ns. Virtual Machine Manager (VMM), joka on 32-bittinen ja toimii prosessorin suojatussa moodissa /9/. Sen pääasiallinen tehtävä on luoda, suorittaa, valvoa ja tuhota virtuaalikoneita. VMM tarjoaa palvelut, joilla hallitaan muistia, prosesseja, keskeytyksiä ja virhetilanteita. Se hyödyntää virtuaaliajureita, joiden kautta sovellusohjelmat pystyvät käyttämään laitteistoa ja käyttöjärjestelmän tarjoamia palveluita.

Toisin kuin Windows 3.1:ssä, Windows 95:ssa sekä VMM että virtuaaliajurit toimivat samassa 32-bittisessä muistialueessa suojaustasolla 0 (Kutsutaan usein ring 0:ksi). Tällä tarkoitetaan sitä että niillä on rajoittamaton oikeus käsitellä koneen resursseja ja muistia.

VMM tarjoaa monisäikeisen, keskeyttävän moniajon. Eri sovellusohjelmat toimivat kukin eri virtuaalikoneessa, ja VMM pystyy suorittamaan samanaikaisesti useita sovellusohjelmia jakamalla prosessorin aikaa eri koneiden välillä.

Virtuaaliset ajurit (Virtual devices, Vxd:t) ovat 32-bittisiä ohjelmia, jotka mahdollistavat laiteriippumattoman VMM:n toiminnan, tarjoamalla rajapinnan eri laitteiden välille. VxD:t tukevat kaikkia tyypillisiä laitteistoja, mukaanlukien ohjelmoitavan keskeytys-kontrollerin, ajastimet, DMA-ohjaimet (Direct memory access), kovalevyajurit, sarjaportit, rinnakkaisportit, näppäimistöt ja näytönohjaimet. Jokaisella laitteella on oltava oma VxD, jonka kautta laitetta käsitellään, ja jossa ne voivat säilyttää itselleen tärkeää tietoa.

### *Windows 95 ja DOS-ohjelmat*

Windows 95 tukee DOS:lle kirjoitettuja ohjelmia. Jokainen käynnistetty DOS ohjelma saa käyttöönsä oman erillisen virtuaalikoneen (VM). Virtuaalikone voi suorittaa DOS ohjelmaa joko prosessorin virtuaalisessa 8086-tilassa tai suojatussa tilassa.

Useimmat DOS-ohjelmat toimivat hyvin yhtäaikaa Windows 95 kanssa, mutta tarjotakseen mahdollisimman hyvän yhteensopivuuden Windows 95 on mahdollista käynnistää erityisessä DOS-tilassa.

DOS-tilassa Windows 95 suorittaa vain yhtä Dos-ohjelmaa kerrallaan. Windows-ohjelmien suorittaminen ei ole mahdollista, eikä esimerkiksi graafista käyttöliittymää käynnistetä.

## *Windows 95 ja 16-bittiset Windows ohjelmat*

Windows 95 tukee myös vanhoja 16-bittisiä ohjelmia. Vanhojen ohjelmien toimimista varten Windows 95 ylläpitää yhteistoiminnallisen moniajon mallia. Kaikki 16-bittiset Windows ohjelmat jakavat saman virtuaalikoneen, osoiteavaruuden, viestijonon ja suoritussäikeen. Virheellisesti käyttäytyvä 16-bittinen ohjelma pystyy siis helposti rikkomaan myös Windows 95:n.

### *Windows 95 ja NT*

Kaikkien Windows 95:ssä toimivien ohjelmien pitäisi toimia myös NT:ssä. NT tarjoaa kuitenkin hyvät turvallisuusominaisuudet, jotka puuttuvat Windows 95:sesta. Yhteensopivuussyistä samat funktiot kyllä löytyvät molemmista, mutta Windows 95:ssä ne eivät tee mitään. Puuttuvia ominaisuuksia ovat useat turvallisuus- ja tapahtumienseurantatoiminnot.

### *Windows 95 ja turvallisuus*

Windows 95 on huomattavasti lähempää sukua Windows 3.1:lle kuin Windows NT:lle, niinpä Windows 95 ei pysty korjaamaan useimpia Windows 3.1:n turvallisuuspuutteita. Käyttäjien autentikointi ei edelleenkään ole pakollista. Windows 95:stä löytyy kyllä asetus, jolla käyttäjän on pakko kirjottautua sisälle palvelimeen, ennen kuin hän pääsee käyttämään työasemaa. Ongelman aiheuttaa se että Windows 95 on mahdollista aina käynnistää niin kutsutuun turvatilaan (safe-mode), jossa tätä sisäänkirjottautumista ei vaadita. Lisäksi turvatilassa on mahdollista kytkeä pakollisen sisäänkirjottautumisen vaatimus pois päältä.

Koska turvallisuuden kannalta Windows 95 on hyvin lähellä Windows 3.1:stä, DeskTop pystyy tarjoamaan 95:seen lähestulkoon saman toiminnallisuuden kuin mitä se tarjoaa Windows 3.1:seen. Tiedosto-oikeudet ovat 95:sessa aivan yhtä huonot kuin Windows 3.1:ssä. Konfiguraationhallinnan ongelmat ovat Windows 95:ssa käytännössä samat kuin Windows 3.1:ssä. DeskTop:in siirtäminen Windows 95:seen on luultavasti varsin suoraviivainen toimenpide.

# 7. Tulevaisuuden näkymiä

Windows 3.1:nen poistuu ajanmittaan markkinoilta. Samalla DeskTop:in kohdeympäristö poistuu. Uudet käyttöjärjestelmät kuten Windows 95 tai Windows NT eivät kuitenkaan pysty tarjoamaan samaa toiminnallisuutta kuin DeskTop. Nykyinen DeskTop on kuitenkin varsin tiukasti sidottu Windows 3.1:sen rakenteeseen. Jos DeskTop halutaan tuoda NT ja Windows 95 ympäristöihin, joudutaan sitä muuttamaan varsin paljon.

NT ja Windows 95 käyttävät yhteistä Windows 32bit ohjelmointirajapintaa, joten olisi hyvä jos DeskTop:sta pystyttäisiin käyttämään mahdollisimman paljon samoja komponentteja molemmissa käyttöjärjestelmissä.

NT:ssä turvallisuusasiat on toteutettu hyvin ja niiden parantamiseen ei ole juurikaan tarvetta. Turvallisuusmielessä DeskTop voi NT:hen lähinnä tarjota tuen toimikorteille. Sen sijaan konfiguraatioiden hallintaan NT ei tarjoa mitään merkittävää. Käyttäjien konfiguraatiot ovat konekohtaisia, eikä niitä siirretä automaattisesti käyttäjien mukana. Konfiguraatioiden hallinta on varsin samalla tasolla sekä NT:ssä että Windows 95:sessa. DeskTop voisi tarjota molempiin parempaa hallittavuutta, käyttäjien konfiguraatioiden automaattista siirtämistä koneesta toiseen sekä ohjelmien automaattista asentamista.

DeskTop on hyvin voimakkaasti yrityskäyttöön suunnattu ohjelmisto. Se on parhaimmillaan ympäristöissä jotka ovat keskitetyisti hallittuja. Ympäristöjä missä ylläpitäjät huolehtivat koko tietojärjestelmästä ja sen toiminnasta. Yritysmaailman lisäksi toinen hyvin suuri asiakasryhmä, jolla olisi käyttöä turvallisuudelle ja konfiguraationhallinnalle olisi kotikäyttö. Windows on käytössä myös kotona ja siellä ei aina ole käytettävissä asiantuntijaa joka osaisi korjata rikkoutuneen konfiguraation. Lisäksi käyttäjät ovat usein esimerkiksi lapsia. Windowsin konfiguraation rikkoo helposti tahattomasti esimerkiksi File Managerilla. DeskTop voisi tarjota myös koteihin tietoturvaa, ja mahdollistaa koneen turvallisen käytön.

# 8. Yhteenveto

Tietokoneilta vaaditaan yhä suurempaa toimintavarmuutta. Ei voi olla hyväksyttävää, että tietojärjestelmät toimivat epäluotettavasti. Toimintavarmuuden ja turvallisuuden vaatimukset kohdistuvat erityisesti käyttäjärjestelmiin. Käyttöjärjestelmät ovat se perusta, jonka päälle sovellukset kootaan.

Microsoft Windows on saavuttanut hallitsevan markkinaosuuden. Se on yleisesti hyväksytty mikrotietokoneiden käyttöjärjestelmäksi. Windows itse ei tällä hetkellä pysty vastaamaan turvallisuusvaatimuksiin, mutta epäilemättä tulevaisuudessa markkinoiden vaatimuset tulevat ohjaamaan kehitystä niin, että myös tavallisen toimistokäytössä olevan käyttöjärjestelmän on oltava turvallinen.

DeskTop täyttää hyvin sille asetetut vaatimukset. Sille on olemassa tarve lähes kaikissa mikrotietokone ympäristöissä. Se mahdollistaa keskitetyn ylläpitämisen, työasemien jakamisen ja konfiguraatioiden seuraamisen koneesta toiseen. Samalla se nostaa Windows-työasemien turvallisuustasoa. Tuloksena on stabiilimpi ympäristö, käyttäjät voivat luottaa enemmän siihen että tietokoneet pysyvät käyttökunnossa, ja että he eivät omilla toimillaan pysty saattamaan Windowsia epästabiiliin tilaan. Ylläpitäjille DeskTop tarjoaa keskitettyä ylläpitoa ja sitä kautta ajan säästöä ja työmäärän pienenemistä.

Työn tekemisen kannalta oman mielenkiintoisen sivujuonen tarjosi NetWare:n hakemistopuu. Konfiguraationhallinnalle käyttäjä ja käyttäjäryhmien jakautuminen eripuolille hakemistopuuta aiheutti mielenkiintoisia ongelmia.

DeskTop on ollut markkinoilla nyt pari kuukautta ja se on saanut hyvän vastaanoton. Ylläpitäjille konfiguraationhallinta on osoittautunut haastavaksi ja mielenkiintoiseksi kokonaisuudeksi. Ylläpitäjien on joskus vaikea tietää mihin kaikkeen tehdyt muutokset vaikuttavat. Tämä asettaa dokumentoinille ja käyttöliittymille lisää haasteita.

DeskTop projektina jatkuu ja seuraavana on vuorossa luultavasti versio Windows 95:selle tai NT:lle.

# Lähdeluettelo

1. Deborah Russel & G.T Gangemi Sr. 1992. Computer Security Basics. USA, O'Reilly & Associates INC. 448 s.

2. ITSEC. 1992. Information Technology Security Evaluation Criteria. Commission of the European Communities. 164 s.

3. A Silberschatz, J Peterson, P Galvin, 1991, Operating System Concepts 3rd edition, Addisson Wesley, USA 696

4. Matt Pietrek, 1993, Windows Internals, USA, Addison-Wesley. 525 s

5. Novell. 1991. NetWare Version 3.11 Concepts, USA, Novell, 280 s.

6. Novell. 1994. NetWare 4, 4.1 Online Documentation, USA, Novell, cd-rom.

7. Helen Custler, Inside Windows NT, USA, Microsoft Press 382s

8. Helen Custer.1994. Inside the Windows NT File System. USA, Microsoft Press. 91 s.

9. Microsoft. 1995. Programmer's Guide to Microsoft Windows 95, USA, Microsoft Press, 674 s.

10. Andrew Schulman, David Maxey, Matt Pietrek, 1992, Undocumented Windows, USA, Addison-Wesley. 715 s

11. Jennifer Seberry, Josef Piprzyk, 1989, Cryptography, An Introduction to Computer Security, Prentice Hall, Australia, 375s